Supplemento ordinario alla "Gazzetta Ufficiale,, n. 169 del 21 luglio 2000 - Serie generale

Spediz. abb. post. 45% - art. 2, comma 20/b
Legge 23-12-1996, n. 662 - Filiale di Roma

GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA

PARTE PRIMA **Roma - Venerdì, 21 luglio 2000** SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DIREZIONE E REDAZIONE PRESSO IL MINISTERO DELLA GIUSTIZIA - UFFICIO PUBBLICAZIONE LEGGI E DECRETI - VIA ARENULA 70 - 00100 ROMA
AMMINISTRAZIONE PRESSO L'ISTITUTO POLIGRAFICO E ZECCA DELLO STATO - LIBRERIA DELLO STATO - PIAZZA G. VERDI 10 - 00100 ROMA - CENTRALINO 06 85081

N. 116

MINISTERO DELL'INTERNO

DECRETO MINISTERIALE 19 luglio 2000.

Regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici.

SOMMARIO

MINISTERO DELL'INTERNO

DECRETI, DELIBERE E ORDINANZE MINISTERIALI

MINISTERO DELL'INTERNO

DECRETO 19 luglio 2000.

Regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici.

IL MINISTRO DELL'INTERNO

Visto l'art. 2 della legge 15 maggio 1997, n. 127, come modificato dall'art. 2, comma 4, della legge 16 giugno 1998, n. 191;

Visti il regio decreto 18 giugno 1931, n. 773 ed il regio decreto 6 maggio 1940, n. 635;

Vista la legge 31 dicembre 1996, n. 675;

Visto il decreto del Presidente del Consiglio dei Ministri 22 ottobre 1999, n. 437;

Sentita l'Autorità per l'informatica nella pubblica amministrazione;

Sentita la Conferenza Stato-città ed autonomie locali, che ha espresso il proprio avviso nella riunione del 22 giugno 2000;

Decreta:

Capo I

PRINCIPI GENERALI

Art. 1.

Definizioni

1. Ai sensi del presente decreto si intende:

a) per «D.P.C.M.»: il decreto del Presidente del Consiglio dei Ministri del 22 ottobre 1999, n. 437;

b) per «documento»: la carta d'identità elettronica e/o il documento d'identità elettronico di cui all'art. 2 del decreto del Presidente del Consiglio dei Ministri costituito dall'insieme del supporto fisico e dei supporti informatici;

c) per «S.S.C.E.»: il sistema di sicurezza del circuito di emissione dei documenti;

d) per «S.A.I.A.»: il sistema predisposto dal Ministero dell'interno per l'accesso e l'interscambio anagrafico;

e) per «Istituto»: l'Istituto Poligrafico e Zecca dello Stato;

f) per «dati»: i dati identificativi della persona di cui all'art. l, comma 1, lettera *d)* e gli altri elementi di cui all'art. 3, comma 1, lettere da *b)* ad *h)*, del D.P.C.M.;

g) per «carta-servizi»: l'insieme dei dati di cui alla precedente lettera *f)* - ad esclusione della fotografia e della firma - e delle informazioni amministrative di cui all'art. 1, comma 1, lettera *e)* e dell'art. 3, comma 4, del D.P.C.M.;

h) per «codice cifrato»: la coppia di codici alfanumerici che identificano univocamente il microprocessore di ogni documento;

i) per «cartellino elettronico»: la trasposizione, in formato digitale e cifrata, del cartellino cartaceo di cui all'art. 290 del regio decreto 6 maggio 1940, n. 635;

j) per «P.I.N.»: il numero identificativo personale necessario alla fruizione dei servizi che ne richiedono l'utilizzo.

Art. 2.

Funzioni dei comuni

1. Le funzioni di pertinenza dei comuni possono essere esercitate anche in forma associata.

2. I comuni, nel rispetto delle regole tecniche e di sicurezza di cui all'allegato B al presente decreto, predispongono in piena autonomia i servizi locali.

Art. 3.

Modalità di connessione

1. Le amministrazioni e gli enti che, ai sensi della normativa vigente e del D.P.C.M., esercitano funzioni e svolgono compiti nell'ambito delle procedure di produzione, trasmissione, formazione, rilascio, rinnovo, aggiornamento e relativa verifica dei documenti si connettono al S.S.C.E. con le modalità di cui all'allegato B e devono provvedere all'aggiornamento dell'indice delle anagrafi tramite collegamento al S.A.I.A.

Art. 4.

Misure di sicurezza

1. Ai fini della produzione, del rilascio, dell'aggiornamento e del rinnovo dei documenti, il trattamento dei dati, da parte delle amministrazioni e degli enti indicati dall'art. 3, comma 1, è effettuato nel rispetto dell'art. 15 della legge 31 dicembre 1996, n. 675 e delle disposizioni di cui al decreto del Presidente della Repubblica 28 luglio 1999, n. 318, nonché delle ulteriori prescrizioni tecniche descritte nell'allegato B.

Art. 5.

Servizi e modalità di autenticazione

1. Ai sensi dell'art. 3, comma 4, e dell'art. 7, comma 1, del D.P.C.M., tutti i servizi che non implicano la memorizzazione dei dati sui documenti sono predisposti in piena autonomia dalle amministrazioni. Le modalità di autenticazione in rete per l'accesso ai servizi da parte del titolare del documento sono definite nell'allegato B.

2. Per i servizi che richiedono la memorizzazione di dati sui documenti è necessaria l'installazione degli stessi da parte del comune e, qualora relativi a dati sensibili, la richiesta dell'interessato.

3. I servizi nazionali che richiedono la memorizzazione di dati sui documenti sono predisposti con le modalità e nel rispetto delle regole tecniche di cui all'allegato B.

Capo II

REGOLE TECNICHE DI BASE

Art. 6.

S.S.C.E. e software di sicurezza

1. In attuazione dell'art. 8, commi 1 e 4, del D.P.C.M. il Ministero dell'interno - Dipartimento della pubblica sicurezza, mette a disposizione delle questure e dei comuni l'infrastruttura organizzativa, informatica e di rete del Centro elaborazioni dati della Polizia scientifica per la realizzazione, la gestione e la manutenzione del S.S.C.E., nonché fornisce ai comuni un software di sicurezza finalizzato a garantire l'integrità, l'accessibilità e la riservatezza delle informazioni nelle fasi di compilazione, rilascio, aggiornamento, rinnovo e verifica dei documenti.

2. Ai sensi dell'art. 6, comma 1, del D.P.C.M. le questure, nei casi previsti dallo stesso articolo, procedono all'interdizione dell'operatività del documento secondo le modalità descritte nell'allegato B.

3. Le questure, ai sensi dell'art. 290 del regio decreto 6 maggio 1940, n. 635, conservano il cartellino elettronico, a cui accedono in via esclusiva, relativo ai documenti rilasciati dai comuni della stessa provincia.

Art. 7.

Supporto fisico

1. Il supporto fisico del documento è costituito da una carta plastica conforme alle norme ISO/IEC 7816-1, 7816-2 e ISO/ID-001 ed è integrato dai supporti informatici di cui all'art. 8.

2. Il supporto fisico è stampato con le tecniche tipiche della produzione di carte valori ed è dotato degli elementi fisici di sicurezza atti a consentire il controllo dell'autenticità del documento visivamente e mediante strumenti portatili e di laboratorio.

3. Il documento ha le caratteristiche grafiche di cui al modello approvato con il presente decreto e di cui all'allegato A.

Art. 8.

Supporti informatici

1. Il supporto fisico di cui all'art. 7 è dotato di una banda ottica per la memorizzazione, con modalità informatiche di sicurezza, dei dati riportati graficamente sul documento, nonché di un microprocessore per la memorizzazione della carta-servizi e per le operazioni connesse alle procedure di identificazione in rete del titolare del documento. Gli standard internazionali, le caratteristiche tecniche e l'architettura logica dei predetti supporti informatici sono conformi alle specifiche indicate nell'allegato B.

Art. 9.

Inizializzazione del documento

1. L'Istituto, cui è riservata la produzione dei documenti a norma dell'art. 11 del presente decreto, provvede alla inizializzazione delle componenti fisiche ed informatiche del documento secondo le procedure di sicurezza descritte nell'allegato B. A seguito della inizializzazione il documento acquisisce la qualità di documento in bianco.

Art. 10.

Configurazione hardware e software
per la formazione del documento

1. Ai fini della formazione dei documenti, i comuni utilizzano la configurazione hardware descritta nell'allegato B.

2. Ai fini della compilazione, rilascio, aggiornamento e rinnovo dei documenti i comuni utilizzano il software di sicurezza di cui all'art. 6, comma 1.

Capo III

Norme procedimentali

Art. 11.

Produzione del documento

1. La produzione del documento è riservata all'Istituto che vi provvede ottemperando alle norme che disciplinano la produzione delle carte valori e dei documenti di sicurezza della Repubblica italiana e agli standard internazionali di sicurezza previsti per l'emissione di carte di pagamento.

2. Nella fase di produzione a regime dei documenti elettronici di cui al presente decreto, l'Istituto, nell'ambito di proprio stabilimento, costituisce uno speciale settore con accesso limitato ai dipendenti addetti alle specifiche lavorazioni e sorvegliato dalle Forze di polizia, dotato altresì delle sicurezze fisiche antieffrazione e dei sistemi di sorveglianza elettronici definiti di intesa con il Ministero dell'interno.

Art. 12.

Trasmissione del documento in bianco in periferia
e sua custodia da parte del comune

1. La trasmissione alle prefetture dei documenti in bianco è effettuata dal Provveditorato generale dello Stato, d'intesa con l'Istituto, in condizioni di sicurezza, mediante affidamento dei plichi a vettori specializzati nel trasporto di valori.

2. Il comune adotta ogni idonea misura per la custodia dei documenti in bianco in condizioni di sicurezza.

Art. 13.

Procedura di sicurezza per la formazione
e rilascio del documento

1. La formazione ed il rilascio del documento avvengono nel rispetto della seguente procedura di sicurezza:

a) il comune, utilizzando le funzionalità del software di sicurezza di cui all'art. 10, comma 2, genera un messaggio informatico cifrato, costituito dai dati del richiedente e dal codice cifrato necessario all'identificazione in rete del documento e lo invia telematicamente al S.S.C.E.;

b) i dati, ad eccezione del codice fiscale e del numero identificativo del documento, vengono registrati cifrati dal S.S.C.E.; l'accesso ai predetti dati in chiaro è consentito esclusivamente alla questura territorialmente competente;

c) il comune, ricevuta la necessaria abilitazione ad emettere il documento da parte di S.S.C.E., riporta i dati identificativi della persona sul microprocessore e sulla banda ottica secondo le modalità indicate nell'allegato B ed effettua la stampa di tali dati sul supporto fisico;

d) il comune genera il P.I.N., lo stampa su carta chimica retinata in grado di garantire la riservatezza dell'informazione e lo consegna, insieme al documento, al titolare.

2. In via transitoria, i comuni possono avvalersi dell'Istituto ai fini della formazione del documento, utilizzando una configurazione hardware conforme ad uno standard minimo corrispondente alle dotazioni descritte nell'allegato B. In tali casi il software di sicurezza provvede ad inoltrare all'Istituto il messaggio informatico di cui al comma 1, lettera *a)*. L'Istituto non conserva traccia dei dati utilizzati per la formazione del documento.

3. L'Istituto assicura livelli di servizio che consentono la disponibilità presso le prefetture dei documenti formati entro il termine di venti giorni successivi alla ricezione del messaggio informatico di cui al comma 2.

Capo IV

Sperimentazione

Art. 14.

Avvio della fase di sperimentazione

1. I comuni che intendono partecipare alla fase di sperimentazione prevista dall'art. 9 del D.P.C.M. presentano il relativo progetto al Ministero dell'interno.

2. I progetti di cui al comma 1 devono contenere:

a) l'indicazione della data di inizio e della durata della sperimentazione e del responsabile del progetto;

b) la descrizione delle modalità organizzative in rapporto alla dimensione territoriale della sperimentazione e alla stima del quantitativo, effettuata su base presuntiva, dei documenti da rilasciare nel periodo di sperimentazione;

c) la descrizione delle procedure di gestione e dei flussi di dati con specifico riferimento alle modalità di connessione di cui all'art. 3, la descrizione delle procedure di sicurezza, la descrizione delle procedure di controllo;

d) l'analisi dei rischi e la descrizione delle relative contromisure, con specifico riferimento a quelle destinate a prevenire la perdita accidentale delle informazioni trattate;

e) l'indicazione dei servizi da erogare relativamente alla carta-servizi.

3. La sperimentazione è autorizzata ai sensi dell'art. 9 del D.P.C.M. in relazione al numero di carte disponibili, tenendo conto dell'ordine cronologico di presentazione dei progetti di sperimentazione.

4. Il Ministero dell'interno può chiedere che il progetto di sperimentazione venga modificato o integrato. In tal caso si applica la disposizione dell'art. 9, comma 3, secondo periodo, del D.P.C.M.

Art. 15.

Relazione sullo stato della sperimentazione

1. Il responsabile del progetto trasmette, con cadenza bimestrale, al Ministero dell'interno relazioni sullo stato di avanzamento della sperimentazione.

2. Il Ministero dell'interno trasmette copia del progetto di sperimentazione e delle relazioni sullo stato di avanzamento della sperimentazione al Comitato di monitoraggio previsto dall'art. 10 del D.P.C.M.

Roma, 19 luglio 2000

Il Ministro: Bianco

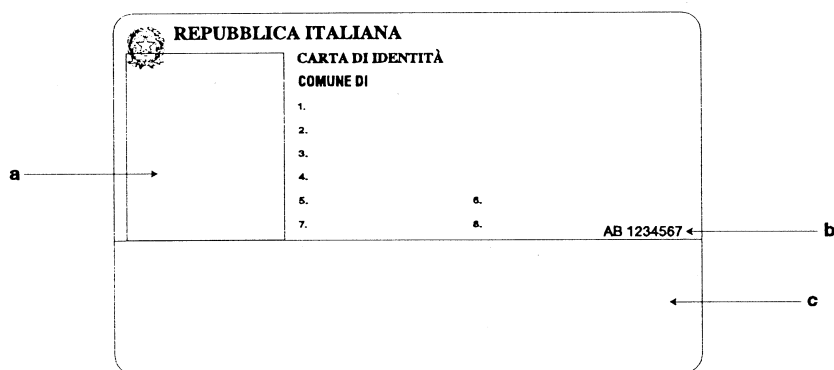
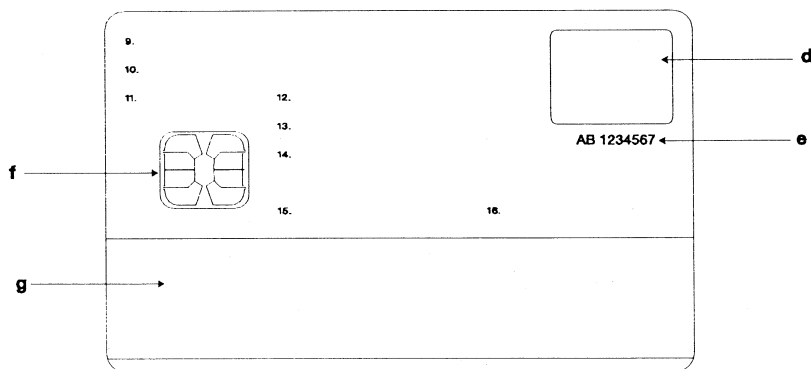
ALLEGATO A

VERSIONE ITALIANO

LEGENDA:

1 = COMUNE CHE RILASCIA IL DOCUMENTO
2 = COGNOME DEL TITOLARE
3 = NOME DEL TITOLARE
4 = COMUNE DI NASCITA
5 = DATA DI NASCITA
6 = SESSO
7 = ESTREMI ATTO DI NASCITA
8 = STATURA (in cm)
a = fotografia del titolare (dimensioni 23x28 mm)
b = numero assegnato al documento in bianco
c = spazio riservato alla codifica ICAO con caratteri OCRB

All. A - FRONTE -

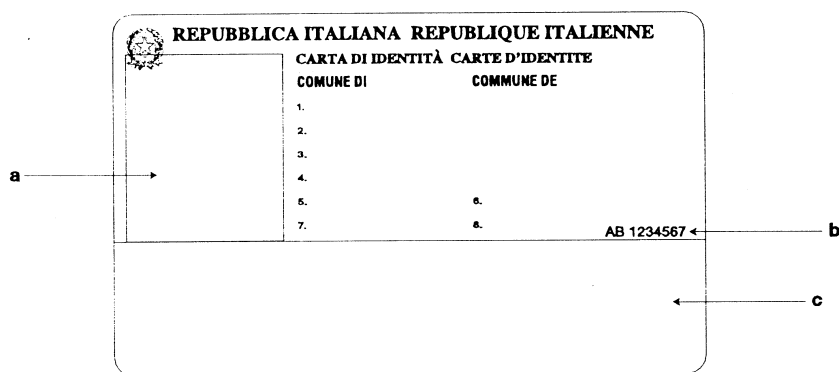
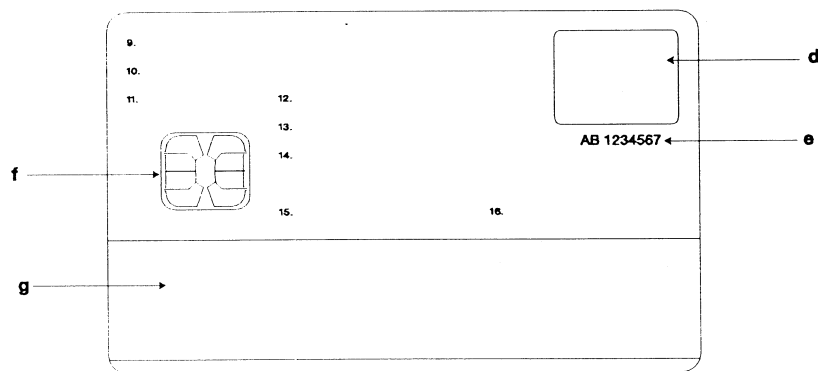
All. A - RETRO -

9 = COMUNE DI RESIDENZA
10 = INDIRIZZO
11 = DATA EMISSIONE DOCUMENTO
12 = DATA SCADENZA DOCUMENTO
13 = CITTADINANZA
14 = CODICE FISCALE
15 = FIRMA
16 = INDICAZIONE DELLA VALIDITÀ PER L'ESPATRIO
d = ologramma (dimensioni 18x14 mm)
e = numero assegnato al documento in bianco
f = modulo CHIP
g = banda a memoria ottica

VERSIONE ITALIANO/FRANCESE

LEGENDA:

1 = COMUNE CHE RILASCIA IL DOCUMENTO
2 = COGNOME DEL TITOLARE
3 = NOME DEL TITOLARE
4 = COMUNE DI NASCITA
5 = DATA DI NASCITA
6 = SESSO
7 = ESTREMI ATTO DI NASCITA
8 = STATURA (in cm)
a = fotografia del titolare (dimensioni 23x28 mm)
b = numero assegnato al documento in bianco
c = spazio riservato alla codifica ICAO con caratteri OCRB

All. A - FRONTE -

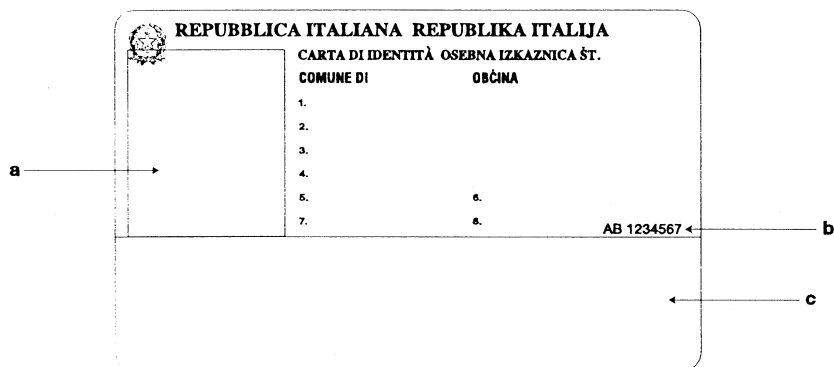
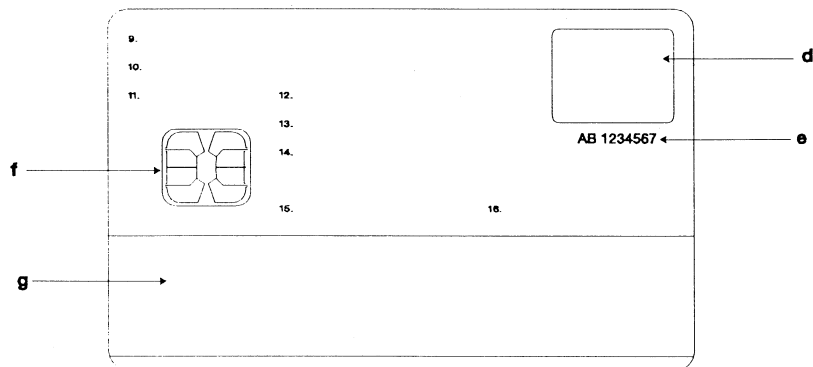
All. A - RETRO -

9 = COMUNE DI RESIDENZA
10 = INDIRIZZO
11 = DATA EMISSIONE DOCUMENTO
12 = DATA SCADENZA DOCUMENTO
13 = CITTADINANZA
14 = CODICE FISCALE
15 = FIRMA
16 = INDICAZIONE DELLA VALIDITÀ PER L'ESPATRIO
d = ologramma (dimensioni 18x14 mm)
e = numero assegnato al documento in bianco
f = modulo CHIP
g = banda a memoria ottica

VERSIONE ITALIANO/SLOVENO

LEGENDA:

1 = COMUNE CHE RILASCIA IL DOCUMENTO
2 = COGNOME DEL TITOLARE
3 = NOME DEL TITOLARE
4 = COMUNE DI NASCITA
5 = DATA DI NASCITA
6 = SESSO
7 = ESTREMI ATTO DI NASCITA
8 = STATURA (in cm)
a = fotografia del titolare (dimensioni 23x28 mm)
b = numero assegnato al documento in bianco
c = spazio riservato alla codifica ICAO con caratteri OCRB

All. A - FRONTE -

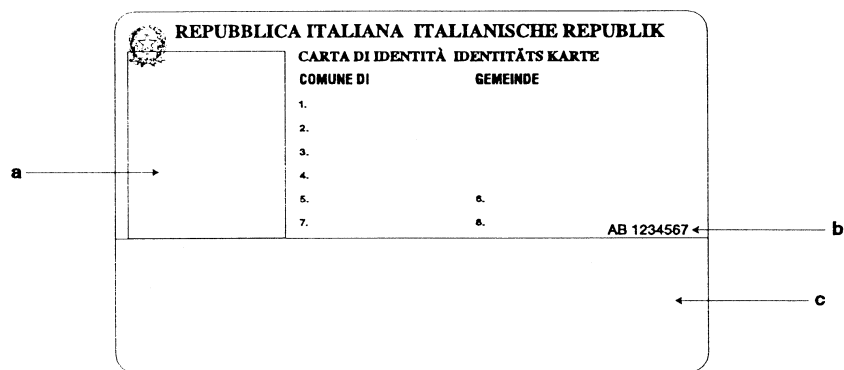
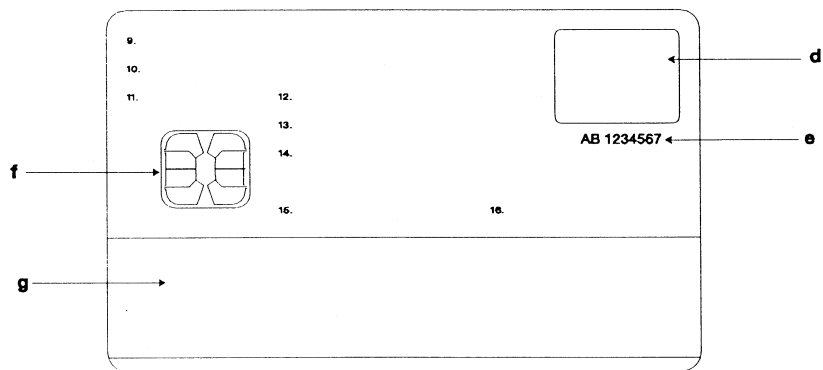
All. A - RETRO -

9 = COMUNE DI RESIDENZA
10 = INDIRIZZO
11 = DATA EMISSIONE DOCUMENTO
12 = DATA SCADENZA DOCUMENTO
13 = CITTADINANZA
14 = CODICE FISCALE
15 = FIRMA
16 = INDICAZIONE DELLA VALIDITÀ PER L'ESPATRIO
d = ologramma (dimensioni 18x14 mm)
e = numero assegnato al documento in bianco
f = modulo CHIP
g = banda a memoria ottica

VERSIONE ITALIANO/TEDESCO

LEGENDA:

1 = COMUNE CHE RILASCIA IL DOCUMENTO
2 = COGNOME DEL TITOLARE
3 = NOME DEL TITOLARE
4 = COMUNE DI NASCITA
5 = DATA DI NASCITA
6 = SESSO
7 = ESTREMI ATTO DI NASCITA
8 = STATURA (in cm)
a = fotografia del titolare (dimensioni 23x28 mm)
b = numero assegnato al documento in bianco
c = spazio riservato alla codifica ICAO con caratteri OCRB

All. A - FRONTE -

All. A - RETRO -

9 = COMUNE DI RESIDENZA
10 = INDIRIZZO
11 = DATA EMISSIONE DOCUMENTO
12 = DATA SCADENZA DOCUMENTO
13 = CITTADINANZA
14 = CODICE FISCALE
15 = FIRMA
16 = INDICAZIONE DELLA VALIDITÀ PER L'ESPATRIO
d = ologramma (dimensioni 18x14 mm)
e = numero assegnato al documento in bianco
f = modulo CHIP
g = banda a memoria ottica

ALLEGATO B

Indice dei contenuti

1. Introduzione

1.1 Bibliografia di riferimento e standard utilizzati

- Schema per il circuito di emissione della Carta di Identità elettronica, Roma 22 dicembre 1999 – AIPA /Associazioni dei fornitori – Gruppo di lavoro Carta d'Identità Elettronica;
- Processo di autenticazione in rete. Roma 22 dicembre 1999 – AIPA /Associazioni dei fornitori – Gruppo di lavoro Carta d'Identità Elettronica;
- CCITT X 208 per le Abstract Sintax Notation One(ASN.1);
- CCITT X 209 per le Basic Encoding Rules (BER) della sintassi ASN.1;
- RSA Laboratories Technical Notes : A Layman's Guide to a Subset of ASN.1 , BER and DER (Distinguished Encoding Rules);
- CCITT X509 versione 3 per il formato dei Certificati Digitali, le estensioni e le policy;
- 2 FIPS 180-1 per la funzione di Hash SHA-1;
- FIPS 46 per il Data Encryption Standard;
- RSA 78 Rivest,Shamir,Aldeman. A method for obtaining digital signatures and public key Cryptosystems;
- PKCS#1 per il formato dei dati da sottoporre ad autenticazione;
- PKCS#7 per la sintassi dei dati da sottoporre ad autenticazione;
- PKCS#9 per i "selected attribute type " da utilizzare nella sintassi PKCS#7 e PKCS#10;
- PKCS#10 per la sintassi delle richieste di certificazione di chiavi pubbliche;
- ISO/IEC 11694-1-2-3-4 Annex A e Annex B per la parte relativa alla banda ottica;
- ISO/IEC 7816-1-2-3-4-5-6-7-8-9 per la parte relativa al microchip.

1.2 Struttura della carta

La carta d'identità elettronica (**CIE**) è una carta ibrida, in grado di integrare nel supporto fisico sia una banda a memoria ottica che un microprocessore.

La banda ottica a lettura laser è utilizzata per la memorizzazione dei "dati" identificativi (D.M. Art. 1, comma 1, lettera f) ai fini della salvaguardia delle esigenze di pubblica sicurezza. L'elevata capacità di memoria disponibile, utilizzata per la memorizzazione di immagini o di informazioni di grosso volume, associata alla capacità elaborativa del microchip, può consentirne un utilizzo anche per la fruizione di servizi locali o nazionali.

Il microprocessore è utilizzato per assolvere le funzioni di "carta servizi" (DM Art. 1, comma 1, lettera g), per consentire l'identificazione in rete e, quindi, l'erogazione di servizi telematici.

Le caratteristiche grafiche della CIE (D.M. art. 7, comma 3), unitamente al dettaglio delle informazioni presenti, sono riportate nell'allegato **A**.

2. Infrastruttura organizzativa (fa riferimento all'art.3 del D.M.)

Nel circuito di emissione intervengono gli enti nel seguito descritti:

Fornitori di microprocessori: *Aziende produttrici dei microprocessori.*
Provvedono alla fornitura dei microprocessori, durante la produzione memorizzano, in area non riscrivibile, un codice seriale composto di un numero progressivo, dal lotto e dalla data di produzione. Il numero deve essere univoco. Ogni consegna di lotti di chip, deve essere accompagnata da distinta cartacea ed elettronica dalla quale si evinca il numero di microprocessori consegnati ed i relativi numeri seriali impressi al loro interno.
Acronimo **Fp**

Fornitori di bande laser; *Aziende produttrici della banda ottica a lettura laser.*
Provvedono alla fornitura delle bande ottiche a lettura laser, durante il processo di produzione imprimono, tramite scrittura laser, un codice seriale composto di un numero progressivo, dal lotto e dalla data di produzione. Il numero deve essere univoco. Ogni consegna di lotti di bande ottiche, deve essere accompagnata da distinta cartacea ed elettronica dalla quale si evinca il numero di bande ottiche consegnate ed i numeri seriali impressi al loro interno.
Acronimo **Fb**

Istituto Poligrafico e Zecca dello Stato: *Ente a cui è riservata la produzione del documento.*
Provvede alla manifattura delle carte, all'inserimento (embedding) della banda ottica e del microprocessore nel supporto fisico, nonchè alla inizializzazione elettrica di quest'ultimo.
Memorizza nel chip, ai fini della garanzia di autenticità, nella banda ottica tramite laser e nella banda ottica in modalità "Embedded hologram" il numero d'identificazione univoco su scala nazionale, fornitogli dal Sistema di Sicurezza del Circuito di Emissione, ed inscindibilmente legato ad essa.
Imprime lo stesso numero in maniera grafica sul supporto fisico e stampa gli elementi grafici costanti (logo, sfondo, etc.).
Contabilizza i numeri seriali che identificano il lotto e la data di produzione del chip e della banda ottica.

Trasmette le informazioni risultanti dalle procedure di inizializzazione al Sistema di Sicurezza.
Acronimo **IPZS**

Ministero dell'Interno Sistema di Sicurezza del Circuito di Emissione: *Ente che fornisce le infrastrutture tecnologiche e garantisce la sicurezza dell'intero circuito di emissione*
In attuazione dell'art. 8, comma 4, del DPCM del 22 ottobre 1999, n 437, il Ministero dell'Interno – Dipartimento della

Pubblica sicurezza mette a disposizione l'infrastruttura organizzativa, informatica di rete del Centro Elaborazioni Dati della Polizia Scientifica, per la realizzazione, la gestione e manutenzione del Sistema di sicurezza del circuito di emissione.
Al fine di garantire la sicurezza dell'intero circuito di emissione ha la responsabilità di verificare e certificare qualunque operazione che comporti l'inserimento, la modifica o la cancellazione delle informazioni (in particolare i dati identificativi) memorizzate sul microprocessore o sulla banda ottica, eccezion fatta per i dati relativi alla predisposizione ed erogazione dei servizi.

Ai fini della garanzia di autenticità, genera per ogni carta un numero di identificazione univoco, su scala nazionale, che trasmette all'IPZS.
Tramite collegamenti telematici consente alle singole Questure di accedere ai documenti, conservati in forma cifrata presso il sistema.
Ciascuna Questura, e solo essa, può decrittare i documenti di sua competenza, ovvero quelli rilasciati dai Comuni della stessa Provincia.
Acronimo **SSCE**

Ministero dell'Interno SAIA:

Sistema di Accesso e Interscambio Anagrafico
Sistema di interscambio dati anagrafici tra le procedure informatiche delle diverse Amministrazioni Pubbliche per fornire servizi integrati al cittadino focalizzando sul Comune la registrazione di tutti gli eventi che comportano un aggiornamento delle informazioni anagrafiche riportate nelle diverse banche dati settoriali della P.A..
Acronimo **SAIA**

Emettitore:

Ente responsabile della formazione e del rilascio.
È il Comune al quale il cittadino si rivolge per richiedere la CIE.
Acronimo **E**

3. Infrastrutture tecniche e di rete

3.1 Dotazioni del SSCE (fa riferimento all'art. 6 del D.M.)

Ai fini dell'emissione della CIE, il sistema di sicurezza del circuito d'emissione (SSCE) si compone di:

- connessione alle reti di accesso;
- funzioni di "security service provider" per consentire l'accesso, con modalità di sicurezza, dei Comuni tramite Internet;
- rete digitale delle Questure (già presente) per consentire la visualizzazione e la stampa dei Cartellini Elettronici alle Questure competenti;
- connessione diretta con l'IPZS per l'interscambio d'informazioni nella fase d'inizializzazione;
- software di sicurezza versione server per le funzionalità connesse alle diverse fasi di formazione della CIE.

3.2 Dotazioni dei Comuni

3.2.1 Dotazioni hardware (fa riferimento all'art. 10, comma 1 del D.M.)

Nel seguito è riportata la configurazione di massima degli apparati hardware necessari per la formazione della CIE. Le apparecchiature proposte possono subire variazioni in funzione dell'architettura del sistema informativo dei singoli comuni.

1) Personal Computer di fascia alta;
2) Stampante ad impatto per l'impressione del PIN sulla carta chimica retinata;
3) Lettore/scrittore di banda ottica. Il lettore deve essere provvisto anche di un lettore di microprocessore, al fine di evitare problemi di allineamento delle informazioni.
4) Lettore scrittore di microprocessore;
5) Stampante termografica per l'impressione sul supporto fisico dei dati del titolare. Anche la stampante termografica deve essere provvista di lettore di microprocessore;
6) Scanner per la digitalizzazione della firma e, eventualmente, della fotografia del titolare;
7) Videocamera per la produzione digitalizzata della fotografia del titolare;
8) Scanner per l'assunzione delle impronte digitali. Lo scanner deve acquisire ad una risoluzione di 500 dpi;
9) Apparecchiatura per l'applicazione sul fronte del documento, di un "overlay" di sicurezza..

3.2.2 Dotazioni hardware minimale (fa riferimento all'art. 13, comma 2 del D.M.)

Nel seguito è riportata la configurazione minima degli apparati hardware necessari per la formazione del la CIE in caso il comune si avvalga, in via transitoria, dell'IPZS. Le apparecchiature proposte possono subire variazioni in funzione dell'architettura del sistema informativo dei singoli comuni.

1) Personal Computer di fascia alta;

2) Scanner per la digitalizzazione della firma e, eventualmente, della fotografia del titolare;
3) Videocamera per la produzione digitalizzata della fotografia del titolare;
4) Scanner per l'assunzione delle impronte digitali. Lo scanner deve acquisire ad una risoluzione di 500 dpi;

3.2.3 Dotazioni software applicativo (fa riferimento all'art. 6, comma 1 del D.M.)

I comuni, per le attività inerenti la formazione ed il rilascio delle CIE, saranno dotati di specifico software applicativo di sicurezza, sviluppato e distribuito da SSCE.

Tale software avrà la possibilità di interoperare con i sistemi informativi dei comuni.

3.2.4 Modalità di connessione al Sistema di Sicurezza del Circuito di Emissione (SSCE)

L'interconnessione a SSCE avverrà secondo le seguenti modalità di trasporto:

- tramite rete unitaria della Pubblica Amministrazione (RUPA);
- tramite altre reti a cui sono connesse le amministrazioni locali;
- tramite internet.

In tutti i casi e' necessario l'utilizzo del software di sicurezza versione client.

Il software consente di eseguire le funzioni necessarie per l'acquisizione dei dati del titolare, utili alla formazione del documento, e quelle per operare, con modalità di sicurezza, le connessioni a SSCE.

4. Materiali e standard di riferimento

4.1 Supporto fisico (fa riferimento all'art. 7, comma 1 del D.M.)

4.1.1 Dimensioni nominali e le componenti

Il supporto fisico deve essere conforme alle norme che regolamentano i Documenti di Identità International Standards Organization (ISO)/IEC 7816-1, 7816-2 .

Le dimensioni nominali dovranno essere di 53,98 x 85,6 mm come specificato nella norma ISO/IEC 7810: 1995 per la carta di tipo ID-1. La tolleranza, nelle dimensioni, è quella definita dalla norma stessa.

Lo spessore della CIE, compresi i film di protezione, dovrà essere conforme alla norma ISO/IEC 7810: 1995.

La CIE, sarà costituita da materiali plastici compatibili con gli strumenti tecnologici in essa contenuti, nonchè con i sistemi di personalizzazione utilizzati per la sua compilazione.

La CIE, per un uso normale nel periodo di validità, dovrà rispondere alle specifiche definite:

- nella norma ISO/IEC 7810: 1995 relativamente a: deformazioni, tossicità, resistenza ad agenti chimici, stabilità dimensionale ed inarcamento con temperatura e umidità, inarcamento con l'uso, infiammabilità e durata.

- nella norma ISO/IEC 11693 per la contaminazione, per la trasmissione della luce attraverso lo spessore della carta e per la resistenza agli agenti atmosferici ed ai test di compatibilità con l'ambiente.

Per quanto attiene alla presenza del microchip la CIE, per un uso normale durante il periodo di validità, deve rispondere alle specifiche definite nella norma ISO/IEC 7816 - 1.

L'area a memoria ottica della CIE, per un normale uso durante il periodo di validità, deve rispondere alle specifiche definite dalle norme ISO/IEC 11693, 11694-1, 11694-2, 11694-3, 11694-4.

4.2 Carta a memoria ottica (fa riferimento all'art. 8, comma 1 del D.M.)

La carta ottica è realizzata in policarbonato, un materiale plastico di provenienza aeronautica, 1.000 volte più resistente del PVC, che garantisce un'ottima trasparenza per la scrittura su banda ottica, una elevata resistenza, una maggiore durata nel tempo ed un intervallo termico di utilizzo molto ampio (-40° +100°).

Il film è composto da diversi strati di materiale ed il supporto ottico registrabile è incapsulato tra due livelli di materiale protettivo trasparente che (sulla faccia esterna) è rinforzato da un ulteriore strato "antigraffio".

La capacita' di memoria della carta ottica utilizzata, nella dimensione adottata, è di circa 1,8 MByte.

Ogni carta ottica permette la creazione di settori variabili basati su tracce, consentendo così l'archiviazione di informazioni multiple ed indipendenti.

Le carte ottiche, rispondono allo standard ISO/IEC 11694.

4.3 Microprocessore (fa riferimento all'art. 8, comma 1 del D.M.)

E' composto da un circuito stampato, che esercita le funzioni di interfaccia verso l'esterno, e da un circuito integrato (*chip*), incastonati sulla scheda.

La capacità di elaborazione propria del microcircuito (*chip*), che lo distingue da qualunque altro supporto "passivo", permette di classificare la CIE come una "smart card" (carta intelligente) .

La presenza di un vero sistema operativo e di una memoria riscrivibile e non volatile (EEPROM) rende possibile proteggere i dati memorizzati ed eseguire istruzioni e programmi, in modo del tutto simile ad un vero computer.

La caratteristica, propria del microcircuito, di poter nascondere informazioni all'*esterno* di esso, ed al contempo di poter eseguire istruzioni o programmi *interni*, rende possibile il riconoscimento sicuro della carta per via telematica e la conseguente ed immediata erogazione dei servizi.

In particolare, la presenza del microcircuito sulla carta d'identità elettronica rende possibili:

- l'identificazione sicura, per via telematica, della carta (e del suo titolare) da parte di un server remoto, sede di un servizio erogato;
- l'identificazione, per via telematica, del servizio remoto da parte della carta (il titolare della carta deve essere sicuro che il servizio cui accede - senza poterlo "fisicamente" vedere - sia autentico, altrimenti potrebbe esporre i dati sensibili, memorizzati sulla carta, a lettura non autorizzata o addirittura a contraffazione non rilevata);
- la possibilità di stabilire un canale sicuro di comunicazione tra la CIE ed il server remoto attraverso la cifratura delle informazioni. Il canale cifrato deve quindi "attraversare" l'applicazione client (ad es. il browser) utilizzata per accedere al servizio, al fine di evitare la possibilità di un "attacco nel mezzo".

La capacità di memoria del microcircui.to, in larga parte offerta dalla sua memoria riscrivibile e non volatile (EEPROM), varia attualmente da 2 a 32 Kb con una rapida evoluzione a 64 Kb.

Per la CIE, è richiesta una memoria EEPROM dalla capacità non inferiore a 16 Kb.

Un'altra caratteristica del microcircuito è la presenza di un coprocessore crittografico, che rende estremamente veloci le operazioni di cifratura e di decifratura. Il motore crittografico presente sulla CIE è in grado di eseguire, in modalità nativa, *almeno* l'operazione di RSA *signature* con chiavi non inferiori a 1024 bit.

Il circuito stampato, che protegge il *chip* dallo sforzo meccanico e dall'elettricità statica, deve essere conforme alla norma ISO 7816-3 che fornisce cinque punti di collegamento per potenza e dati.

Gli standard di riferimento, per il microcircuito e per i comandi del sistema operativo da esso ospitato, sono i seguenti:

- ISO 7816-3

- ISO 7816-4
- ISO 7816-8

I comandi, nella forma di APDU, che devono obbligatoriamente rispettare gli standard citati, sono quelli utilizzati dal middleware crittografico di interfaccia con la carta, le cui specifiche sono discusse nel paragrafo che descrivere il processo di autenticazione in rete.

Fa eccezione il comando per lo scambio delle chiavi di sessione, descritto nella sezione riguardante i servizi, che dovrà essere implementato secondo le specifiche riportate in quel paragrafo.

4.4 Dati (fa riferimento all'art. 13, comma 1, lettera d del D.M.)

Di seguito è riportato il formato elettronico dei dati presenti nella CIE.

Descrizione Campo	Tipo
Numero assegnato al documento in bianco	carattere
Comune che emette il documento	carattere
Data di emissione del documento	carattere data
Data di scadenza del documento	carattere data
Cognome	carattere
Nome	carattere
Data di Nascita	carattere data
Sesso	carattere (M/F)
Statura (cm)	carattere
Codice fiscale	carattere
Cittadinanza	carattere
Comune / Stato estero di Nascita	carattere
Estremi atto di nascita	carattere
Comune di residenza	carattere
Indirizzo	carattere
Firma del titolare	BMP JPG (fattore 5)
Eventuale annotazione in caso di non validità del documento per l'espatrio	Logico
Fotografia 23x28mm – 200dpi – 16 Ml di colori(a 24 bit)	BMP JPG (fattore 5)
Impronta digitale (indice destro) 1"x1" – 500dpi – 256 liv. di grigio	BMP WSQ

La dimensione dei vari campi, indicati nella tabella, sarà definita a seguito della elaborazione delle specifiche di dettaglio.

5. Misure di sicurezza (fa riferimento all'art. 4 del D.M.)

Questo paragrafo descrive le misure adottate, durante tutte le fasi della produzione e dell'utilizzo della CIE, per ottenere i corretti livelli di sicurezza e di interoperabilità della carta.

5.1 Sicurezza del supporto fisico

Nel seguito sono elencati gli elementi utilizzabili per la sicurezza del supporto e per accertarne l'autenticità, anche attraverso il semplice esame visivo.

5.1.1 Elementi di sicurezza grafici e di stampa

E' previsto l'uso dei seguenti elementi di sicurezza, tipici delle carte valori:

- motivi antiscanner ed antifotocopiatura a colori;
- stampa con effetto rainbow (a sfumatura di colore graduale e progressiva);
- motivi grafici multicolore richiedenti elevata qualità di registro di stampa;
- microprint;
- processo di masterizzazione photomask con stampa ad alta risoluzione di immagini direttamente su film ottico;
- embedded hologram (incisione grafica su banda laser);

5.1.2 Inchiostri

Per la stampa è previsto l'impiego di inchiostri dotati di speciali caratteristiche, come quelli fluorescenti (visibili all'ultravioletto), interferenziali e otticamente variabili (OVI - Optical Variable Ink).

5.1.3 Numerazione di serie

La numerazione del documento in bianco, realizzata con sistema ad incisione laser sul fronte del documento, è ripetuta visibilmente sulla banda ottica con il sistema dell' "embedded Hologram", memorizzata al suo interno ed inserita come dato all'interno del microprocessore.

5.1.4 Applicazione di elementi Optical Variable Device (OVD)

Sul retro del documento, nella fase di produzione, è applicato a caldo un ologramma di sicurezza.

Sul fronte del documento, quale ultima fase della personalizzazione, è prevista l'applicazione di overlay olografico.

5.2 Sicurezza della fase di personalizzazione

Al fine di consentire la stampa della CIE presso i Comuni o i Centri Servizi ad un costo contenuto, la tecnica da utilizzare è quella della termografia a colori su policarbonato (eventualmente apponendo uno strato neutro intermedio).

Anche la compilazione grafica sarà uniforme per tutto il territorio nazionale tramite l'utilizzo di caratteri, provenienti da un unico "font" appositamente realizzato per la CIE che verrà distribuito unitamente al software di sicurezza, dal SSCE.

Inoltre, l'apposizione di embedded hologram (incisione grafica su banda laser) consente di replicare, su banda ottica, i dati identificativi del titolare del documento, al fine di rendere più sicura l'identificazione a vista.

Infine, come accennato, al termine della stampa termica, il processo prevede l'applicazione sul fronte di un "overlay" di protezione di 12 micron al fine di offrire ulteriori sicurezze e garantire la durata oltre i cinque anni.

5.3 Affidabilità dei dati

5.3.1 Laser su banda ottica

I dati vengono memorizzati permanentemente sulla banda laser (sistema WORM) in formato digitale e letti/scritti con appositi apparati, detti lettori/scrittori.

Ferma restando l'auspicabile corretta conservazione da parte del titolare della carta, per meglio garantire la leggibilità e la coerenza dei dati nel tempo, la superficie della tessera dovrebbe presentarsi pulita e uniforme (es. possibilmente senza graffi o abrasioni). Comunque i supporti informatici utilizzati offrono garanzie di conservazione dei dati molto elevate; infatti, per quanto attiene ai dati contenuti nella banda laser, è attivo un metodo di identificazione e correzione d'errore che garantisce la ricostruzione delle informazioni digitali eventualmente perse per cause accidentali.

5.3.2 Microcircuito

Esistono due distinti livelli di protezione dei dati conservati nella carta: un livello fisico ed un livello logico. La protezione a livello fisico è gestita dal produttore del *chip* che provvede a *mascherare* sulla carta, in maniera indelebile, il sistema operativo proteggendolo mediante una chiave segreta di cui egli solo è a conoscenza.

Il livello logico è invece gestito sia dall'entità che inizializza la CIE che dall'ente che la personalizza.

Tre sono le tipologie di dati che il microcircuito contiene:

- le informazioni specifiche dell'hw e del sw,
- le informazioni anagrafiche del titolare,
- i dati relativi alla carta servizi, cioè necessari alla fruizione dei servizi erogati da un server remoto.

Per quanto riguarda la prima e la seconda tipologia di dati, la registrazione può avvenire soltanto dopo il superamento di particolari condizioni di test e, una volta effettuata, comporta l'aggiornamento dei diritti di accesso ai dati, al fine di impedirne una successiva cancellazione o modifica.

Relativamente alla terza tipologia i dati possono essere distinti in:

- dati individuali aggiuntivi
- dati relativi ai singoli servizi.

L'accesso a questi ultimi dati è possibile solo dopo il consenso del titolare espresso ordinariamente tramite digitazione di PIN.

I dati individuali aggiuntivi sono informazioni relative al titolare che sono registrate sulla carta, ad integrazione delle informazioni anagrafiche, e che possono essere utilizzate ai fini dell'erogazione dei servizi. Queste informazioni estendono l'identità del titolare, non sono specifiche di un servizio e non sono modificabili a seguito dell'erogazione dei servizi. Vengono registrate o modificate sulla carta esclusivamente dal Comune su esplicita richiesta del titolare e, in pratica, abilitano la carta all'accesso a quei servizi delle amministrazioni locali e centrali la cui erogazione necessita di tali dati.

L'elenco dei dati individuali aggiuntivi è definito ed aggiornato dal Dipartimento della Funzione Pubblica, d'intesa con il Ministero dell'Interno e con l'Associazione Nazionale dei Comuni d'Italia.

I dati relativi ai singoli servizi sono informazioni registrate sulla carta, eventualmente modificabili durante l'erogazione del servizio, e relative ad attributi del titolare della carta che sono funzionali esclusivamente all'amministrazione erogante il servizio.

5.4 Sicurezza del circuito (fa riferimento all'art. 6, comma 1 del D.M.)

La migliore garanzia contro tentativi di falsificazioni e utilizzo di carte rubate si trova nella centralizzazione virtuale prevista dall'architettura del circuito d'emissione della CIE.

In tale logica, il sistema di sicurezza dei documenti traccia tutte le operazioni al fine di garantire il rispetto della normativa vigente sulla riservatezza delle informazioni e dei dati personali, per impedire l'emissione di documenti falsi e per individuare facilmente l'utilizzo fraudolento di documenti rubati e la contraffazione di documenti autentici.

Nel capitolo 7 verranno descritte dettagliatamente tutte le fasi del processo di emissione.

5.4.1 Sicurezza degli accessi ai dati (fa riferimento all'art. 6 del D.M.)

In base al Regolamento di esecuzione del Testo Unico delle Leggi di P.S., oltre al titolare possono accedere alle informazioni contenute nei documenti esclusivamente i Comuni, che emettono le carte d'identità, e le Questure competenti territorialmente. Infatti, sia gli uni che gli altri sono tenuti a conservare copia dei documenti emessi.

Passando da un documento cartaceo ad uno di formato elettronico, anche la copia conservata da Comune e Questura (cartellino cartaceo) diviene di tipo digitale (cartellino elettronico).

Pertanto, a fini di sicurezza e nel rispetto delle norme di legge, la “base dati” comune consente l’accesso e la visualizzazione dei cartellini elettronici al solo Comune di residenza ed alla Questura territorialmente competente.

A tal fine il Sistema di Sicurezza (SSCE) garantisce la tracciabilità di tutte le attività, relative ai dati identificativi, per ogni singolo documento, consentendo di risalire, in qualsiasi momento, alle informazioni di "chi ha fatto cosa e quando", nel rispetto delle attuale normativa, durante tutte le fasi di formazione, compilazione, rilascio, rinnovo ed aggiornamento dei documenti.

Il Sistema di Sicurezza, grazie ad un meccanismo di cifratura basata su algoritmo a chiave asimmetrica, non è in grado esso stesso di accedere ad alcuna informazione di carattere personale che può essere visualizzata, tramite la propria chiave privata, esclusivamente dalla Questura o dal Comune competente.

Da un punto di vista tecnico, i dati sono prima cifrati per mezzo di un algoritmo simmetrico di provata robustezza (ad es. 3DES) con una chiave di lunghezza non inferiore a 128 bit (generata in modalità casuale); quest'ultima, prima di essere distrutta, viene a sua volta cifrata sia con la chiave pubblica della Questura che con quella del Comune e memorizzata assieme all’informazione.

5.4.2 Sicurezza della carta

I rischi di furto e falsificazione delle carte d’identità, con l’adozione del modello elettronico, sono notevolmente ridotti, principalmente in virtù della natura del supporto e delle garanzie di inalterabilità delle informazioni riportate, tanto sul chip che sulla banda ottica.

La banda ottica rappresenta l’elemento centrale della sicurezza per i motivi di seguito riportati.

La caratteristica di base della scrittura WORM (Write Once Read Many) non permette alterazioni, realizzate mediante la cancellazione di dati e la loro sostituzione con altri. Infatti, le informazioni memorizzate non sono cancellabili e riscrivibili. Eventuali aggiornamenti consistono esclusivamente in aggiunte, proprio come avviene per un normale CD-Rom.

In ogni caso esistono le protezioni inserite nell’hardware di scrittura, in dotazione esclusivamente a **E** ed **IPZS,** e di ogni operazione effettuata dal funzionario autorizzato elettronicamente si tiene traccia presso SSCE.

Il controllo a vista della carta, inoltre, è garantito dalla presenza dell’Embedded Hologram che permette di effettuare un’azione di costante validazione dei dati stampati in chiaro e di evidenziarne immediatamente il tentativo di manomissione.

Infine non essendo la banda laser modificabile attraverso campi magnetici, calore (100°), campi elettrici, virus informatici, il suo contenuto è inattaccabile.

Gli eventuali interventi meccanici che modifichino strutturalmente o fisicamente la “card” sarebbero immediatamente visibili.

Relativamente al microchip, questi non permette - grazie alla sicurezza del suo stesso sistema operativo - di modificare o scrivere informazioni se non in presenza di determinate autorizzazioni.

Inoltre tutte le informazioni sensibili, tanto sul chip che sulla banda ottica, sono garantite contro l'alterazione, perché "firmate" digitalmente.

5.4.3 Furto della carta "attivata" o documento in bianco

La carta è in tale stato quando viene spedita da IPZS ai comuni, prima di essere formata e rilasciata.

In questo caso, dal momento che la personalizzazione richiede, per poter aver luogo, l'autenticazione del funzionario nei confronti del sistema e la firma dei dati da parte di appositi apparati contenenti la chiave privata dell'ente, tale eventualità rientra nella tipologia del "rilascio fraudolento" realizzabile solo attraverso l'infedeltà del funzionario stesso le cui attività però, con la citata tracciatura, restano registrate nel Data Base delle approvazioni presso SSCE.

5.4.4 Controlli a vista

L'intero circuito di sicurezza attraverso l'adozione dell'architettura a centralizzazione virtuale consente di innalzare il livello di qualità dei controlli, c.d. a vista, effettuati dalle Forze di Polizia per verificare l'identità delle persone sottoposte ai controlli stessi.

Disporre di un documento particolarmente attendibile consente di eseguire tutte le normali procedure in tempi molto ridotti con indubbio vantaggio per le persone coinvolte.

Le sicurezze adottate durante la fase di inizializzazione del documento, la presenza sulla banda ottica, sotto forma di ologramma, delle stesse informazioni grafiche, lo rendono molto più affidabile del modello cartaceo.

Laddove si volessero approfondire le verifiche, due sono le possibili soluzioni:

- Controllo dei dati autenticati e memorizzati nella banda ottica. Tramite apposito lettore opportunamente inizializzato, in grado di rilevare con certezza l'autenticità del documento
- Controllo delle informazioni presso il SSCE. Le Questure di competenza possono, collegandosi al SSCE, verificare immediatamente, grazie al possesso di opportune chiavi crittografiche, se le informazioni in esso contenute corrispondono con quelle riportate nel documento.

5.4.5 Lista dei documenti interdetti (fa riferimento all'art. 6, comma 2 del D.M.)

In attuazione dell'art. 6, comma 1, del D.P.C.M. del 22 ottobre 1999, n. 437, presso il SSCE è presente un elenco dei documenti interdetti (black-list). Tale elenco è indispensabile per impedire l'operatività della CIE in caso di smarrimento o furto della stessa.

Le procedure da seguire per l'interdizione della carta vengono dettagliatamente descritte nei successivi paragrafi.

5.4.6 Software di sicurezza distribuito ai comuni (fa riferimento all'art. 6, comma 1 del D.M.)

Per procedere alla formazione ed all'emissione dei documenti, i Comuni devono collegarsi al SSCE. In assenza di tale collegamento qualsiasi documento prodotto verrebbe facilmente individuato come falso.

I requisiti per collegarsi al circuito di emissione sono un collegamento telematico, secondo i criteri stabiliti al paragrafo 3.2 del presente documento, e l'adozione di uno speciale software di sicurezza rilasciato dal Sistema di Sicurezza stesso.

Il SSCE curerà l'analisi, lo sviluppo, la distribuzione e la manutenzione del software, per motivi di riservatezza, di interoperabilità e di economicità.

Il software, unitamente alla chiave privata del comune, la prima volta dovrà essere ritirato presso il Ministero dell'Interno. Le release successive, invece, grazie alla disponibilità della chiave privata potranno essere prelevato direttamente via Web.

6. Servizi erogabili in rete (fa riferimento all'art. 5 del D.M.)

Le tipologie dei servizi erogabili possono, in sostanza, ricondursi a due: servizi standard che non necessitano di essere installati sul documento e servizi qualificati che richiedono l'installazione.

L'installazione di un servizio qualificato è il processo mediante il quale viene predisposta sulla carta la struttura dati del servizio, ovvero la chiave pubblica del server dell'ente erogatore od entrambi.

I livelli di sicurezza previsti per l'erogazione dei servizi sono:
- Autenticazione forte (strong authentication) del titolare
- Autenticazione forte del server erogatore (autenticazione esterna)
- Cifratura del canale (secure messaging)

Tali livelli di sicurezza possono essere contemporaneamente presenti; in particolare, il secure messaging implica sempre almeno l'autenticazione forte del server. Per tutti i tre livelli è necessaria la digitazione del PIN.

Nel caso dei servizi standard si accede al servizio con il semplice riconoscimento tramite digitazione del PIN e, laddove necessario, l'utilizzo del certificato della carta per la *strong authentication*.

Richiedono l'installazione sulla carta quei servizi che necessitano di informazioni aggiuntive da memorizzare sul documento. Per questi ultimi l'accesso al servizio avviene solo dopo che il Server che eroga il servizio ha riconosciuto, tramite un meccanismo basato su chiavi asimmetriche, la carta ed eventualmente dopo che quest'ultima ha riconosciuto il Server.

I servizi standard vengono erogati senza alcuna autorizzazione ed in piena autonomia dalle amministrazioni interessate ai titolari di carte e possono utilizzare solo il primo livello di autenticazione (autenticazione forte del titolare).

I servizi qualificati, se erogati da amministrazioni centrali, per poter essere installati devono essere previamente *autorizzati.* Tali servizi possono adottare tutti i livelli di sicurezza precedentemente elencati.
Rientra nei servizi qualificati la firma digitale disciplinata dal DPR 513 del 1997. In questo solo caso, viene abilitata la funzione di generazione delle chiavi di sottoscrizione sottoponendola alle medesime condizioni di autenticazione del server remoto che gestisce l'operazione (possesso della chiave privata (Spri) corrispondente alla chiave pubblica (Spub) del server dell'ente certificatore).

6.1 Le liste dei servizi e la lista delle carte interdette (black-list)

Le liste dei servizi sono indispensabili per poter procedere all'installazione dei servizi qualificati sulla carta. Solo i servizi presenti in tale lista possono essere installati sulla carta.

Le liste dei servizi contengono almeno le seguenti informazioni:

- Identificativo del servizio
- Formato della struttura dati da creare sulla carta (se presente)
- Chiave di autenticazione del server erogatore (Spub)

- Spazio richiesto in EEPROM (memoria) del microcircuito
- Informazioni descrittive del servizio

Esistono due tipologie di liste dei servizi:

- La lista dei servizi nazionali (mantenuta da SSCE)
- Le liste dei servizi comunali (mantenute dai Comuni)

La lista nazionale presso il SSCE e le liste comunali interoperano secondo modalità e standard specifici. La lista nazionale contiene l'elenco dei servizi nazionali e l'elenco dei servizi ultracomunali.
Per servizi ultracomunali si intendono quelli che un Comune rende disponibili al di fuori della sua competenza territoriale
Il software di sicurezza rilasciato ai comuni, al fine dell'installazione dei servizi, deve interoperare sia con la lista nazionale sia con l'eventuale lista comunale.

La predisposizione e la gestione della lista dei servizi comunali è affidata alla responsabilità del comune.

La predisposizione e la gestione della lista dei servizi nazionali è affidata al SSCE. Le amministrazioni centrali che intendono offrire servizi qualificati devono richiedere una autorizzazione al Dipartimento della Funzione Pubblica specificando i motivi per cui si ritiene necessario utilizzare questa tipologia di servizio, le modalità di installazione ovvero aggiornamento (nel caso si tratti di un servizio già esistente) e, in caso di parere favorevole, presentare al SSCE un documento in cui si evidenzia:

- la descrizione del servizio da erogare;
- le modalità tecniche attraverso le quali sarà garantito il servizio;
- l'organizzazione a supporto del sistema di erogazione del servizio.

Presso il SSCE è inoltre mantenuta la lista delle carte interdette (black-list), aggiornata secondo le modalità descritte al capitolo 8. Il SSCE mette a disposizione di tutti coloro che erogano servizi l'acesso telematico alla black-list. Saranno le caratteristiche del servizio che si deve erogare a stabilire la necessità di un accesso alla "black list" delle carte interdette.

6.2 Modalità di riconoscimento in rete

In considerazione dell'architettura definita per la carta d' identità elettronica e dell'utilizzo della componente microchip per il riconoscimento in rete della carta nei confronti di un server applicativo che eroga dei servizi, la soluzione che si è scelta è quella della Strong Authentication che richiede l'utilizzo di funzioni tipiche di una Public Key Infrastructure (SSCE).

6.2.1 Crypto Middleware ed API PKCS#11

IL Crypto Middleware è costituito dalle applicazioni (piattaforme) che SSCE mette a disposizione dei *Client,* che operano su reti aperte, per gestire i servizi di cifratura/decifratura.
Orientativamente, tali piattaforme svolgono le seguenti funzioni:

- Accesso LDAP ai servizi di Directory;

- Gestione in *Cache* della *Cerificate Revocation List*;
- *Parsing* dei Certificati Digitali;
- Costruzione di strutture PKCS#7;
- Richiesta di certificazione di chiavi pubbliche;
- Richiesta di revoca di certificati
- Interfaccia ad alto livello verso le funzioni di cifratura.

Queste piattaforme, a loro volta, poggiano su strati software, o API, che le isolano dai dispositivi di cifratura, tipicamente le Smart Card.

Le API più comunemente usate sono le PKCS#11, le cui caratteristiche salienti sono:
- consentire ai Crypto Middleware di prescindere dai dispositivi che memorizzano chiavi e sviluppano crittografia;
- fornire ai Crypto Middleware una interfaccia standard;
- rendere portabili le applicazioni negli ambienti in cui la crittografia è trattata con queste API.

6.2.2 Processo di Strong Authentication

Questo processo consente la identificazione da remoto della carta per la fruizione dei servizi erogati da una applicazione residente presso una Pubblica Amministrazione Centrale.
Orientativamente, i passi previsti dalla procedura sono:

1. L'applicazione client stabilisce la comunicazione con l'applicazione server.

2. L'applicazione server richiede all'applicazione client il file "C_Carta" contenente il certificato (ID_Carta più la chiave pubblica $K_{pub\ della\ carta}$).

3. L'applicazione client interroga la carta e legge tale file mediante i comandi APDU
SELECT FILE (C_Carta),
READ BINARY.

4. L'applicazione client invia il file "C_Carta" al server.

5. L'applicazione server verifica la validita' del certificato mediante $SSCE_{pub}$ ed estrae da esso ID_Carta e K_{pub}.

6. L'applicazione server genera una stringa di challenge e la invia al client rimanendo in attesa della risposta.

7. L'applicazione client seleziona K_{pri} mediante il comando *MSE(Manage Security Environment)*.
In tal modo K_{pri} e' attivata e verra' usata in tutte le successive operazioni di cifratura effettuate dalla carta.
Mediante il comado PSO (*Perform Security Operation*)la carta esegue la cifratura del *challenge* usando K_{priv} precedentemente attivata, e restituisce all'applicazione *client* la stringa ottenuta. La chiave privata che e' stata generata dalla carta in fase di inizializzazione, risulta invisibile dall'esterno e comunque impossibile estrarla dalla carta.

8. Il client invia al server in attesa il challenge firmato ricevuto dalla carta.

9. L'applicazione server verifica la stringa ricevuta e la confronta con il challenge precedentemente generato.
   Se tale confronto ha esito positivo la carta e' autenticata. A questo proposito è necessario che l'algoritmo di verifica, residente sul server, sia compatibile con quello usato dalla carta per cifrare il challenge.

6.2.3 Comandi di gestione utilizzati dalla Strong Authentication

La norma ISO 7816 parte 4 e parte 8 definisce, oltre alla struttura del File System , anche i comandi per interagire a livello applicativo. Tali comandi sono chiamati APDU (Application Protocol Data Unit).

In funzione dei passi procedurali del processo di Autenticazione sopra descritti, sono individuati i seguenti comandi APDU:

- SELECT FILE, per selezionare l'Elementary File che contiene il certificato della Carta di Identità Elettronica (C_Carta);
- READ BINARY, per leggere il certificato;
- MSE (Manage Security Environment), per attivare la chiave privata di autenticazione;
- PSO (Perform Security Operation), per cifrare il *challenge* da inviare alla applicazione server.

Un approccio che è stato scelto per garantire alle applicazioni di gestire in modo interoperabile la componente microchip della Carta di Identità Elettronica è quello di realizzare una libreria di interfaccia che implementi i comandi descritti precedentemente.

Tale libreria, realizzata da SSCE, metterà a disposizione presumibilmente le seguenti funzioni:

- servizi di amministrazione;
- funzioni di interfaccia verso la CIE;
- identificazione Utente;
- selezione File;
- Read File;
- selezione chiave;
- autenticazione Interna;
- gestione errori ed anomalie.

6.3 Considerazioni sulla interoperabilità

Al momento della scrittura di questo documento, non esistono standard di riferimento che garantiscono l'interoperabilità dei sistemi di crittografia, per cui SSCE, per raggiungere questo obiettivo, ha ritenuto opportuno definire sia l'algoritmo crittografico di autenticazione, sia il formato del messaggio autenticato.

La scelta effettuata è quella di utilizzare RSA come algoritmo di autenticazione e PKCS#1 come formato; di seguito sono esposti i razionali che hanno condotto a questa tipo di soluzione.

6.3.1 Algoritmi

Gi algoritmi asimmetrici comunemente impiegati dalle Smart Card ed idonei per realizzare la autenticazione sono l'algoritmo RSA e l'algoritmo DSA

Questi algoritmi sono onerosi dal punto di vista computazionale e quindi sono realizzati utilizzando un coprocessore aritmetico. La lunghezza della chiave dipende dalla capacita del coprocessore di effettuare moltiplicazioni in modulo. Questo comporta una lunghezza massima di chiave pari al massimo modulo supportato dal coprocessore per l'algoritmo DSA ed una lunghezza massima pari al doppio del modulo per l'algoritmo RSA grazie alla possibilità di utilizzare il Chinese Remaider Theorem.

In virtù delle considerazioni precedenti la scelta effettuata è stata quella dell'algoritmo RSA in quanto consente di:

- poter scegliere tra una vasta gamma di fornitori ;
- estendere, in futuro, la lunghezza della chiave.

6.3.2 Formati

I formati generalmente utilizzati dalla crittografia asimmetrica sono:

- il formato ISO 9796 parte 2;
- il formato PKCS#1.

Il formato ISO 9796-2 è adottato dallo standard EMV per l'autenticazione statica e dinamica.

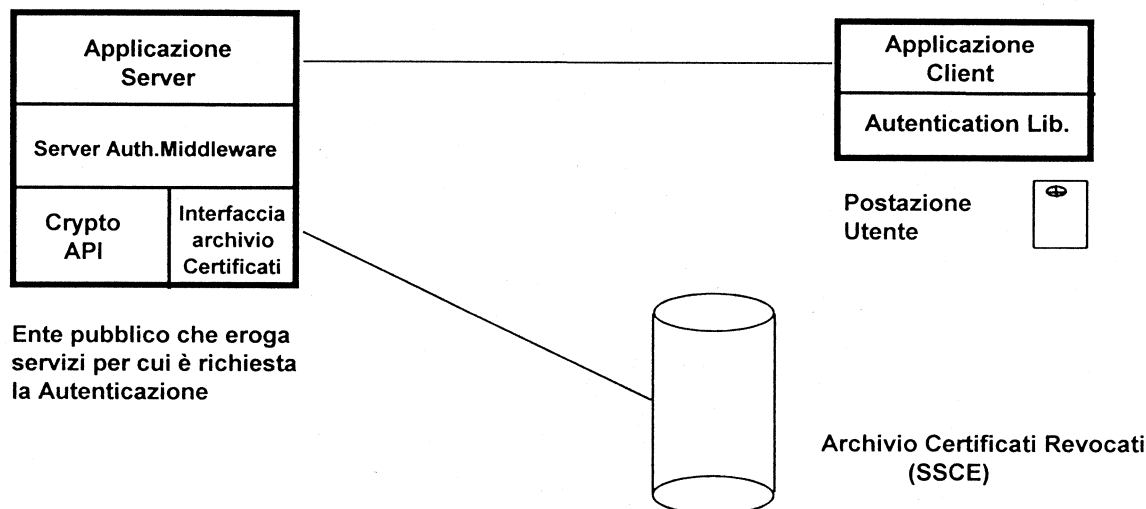
In applicazioni non EMV questo formato è consigliabile quando l'intero processo di autenticazione comporta l'utilizzo di due Smart Card (Mutua autenticazione interna ed esterna).

Il formato PKCS#1 è consigliabile in quanto può essere considerato "standard de facto" ed i messaggi di autenticazione (Response) costruiti secondo questo formato possono essere verificati dalle applicazioni che utilizzano gli strumenti tipici delle Public Key Infrastructure.

6.4 Strong Authentication lato Server

Quanto affermato nei precedenti paragrafi è un solido punto di partenza per risolvere il problema della autenticazione forte in rete per quanto concerne il *Client* e la CIE. E' ora necessario definire la componente server del processo di autenticazione.

La figura [4] illustra i componenti che intervengono nel processo di autenticazione.

Fig. [4]

6.4.1 Server Authentication Middleware

Il Server Authentication Middleware è lo strato software che fornisce i servizi crittografici alla Applicazione.

Le funzioni che questo strato rende disponibili sono:

- Generazione di quantità random;
- Funzioni di Hash;
- Gestione di Certificati digitali in formato X509v3 ;
- Verify Certificate (per validare il certificato della CIE)
- Verify Signature (per validare il messaggio di Autenticazione)
- Caricamento della Certficate Revocation List
- Gestione della Revocation List.

Quelle descritte sono solamente un subset delle funzionalità del Server Authentication Middleware in una Infrastruttura a Chiave Pubblica ma sono comunque sufficienti per considerare la possibilità di utilizzo di software di mercato.

I requisiti di questa componente software sono:

- servizi crittografici come descritto nei punti precedenti;
- interoperabilità con i Client;
- indipendenza degli strumenti di produzione dei certificati.

Il primo requisito è una funzionalità tipica dei *Middleware* crittografici, il secondo requisito è soddisfatto dalla scelta fatta per Algoritmo e Formato che rende univoca la struttura del messaggio di Autenticazione mentre il terzo requisito è garantito dal circuito di emissione della Carta di Identità Elettronica essendo la produzione dei certificati di competenza di SSCE.

6.5 Installazione dei servizi

L'installazione dei servizi avviene durante la fase di formazione e rilascio da parte dei comuni, descritta in maniera analitica nel successivo capitolo 7.

6.6 Aggiornamento dei dati relativi alla fruizione dei servizi

Nei paragrafi precedenti è stato approfondito il tema della autenticazione della CIE verso un Ente in grado di erogare servizi , in questo paragrafo viene completato il processo di autenticazione specificando le procedure che permettono alla CIE di verificare l'autenticità del servizio remoto con cui sta interagendo. Questo processo è chiamato :Autenticazione Esterna

Un altro tema trattato in questo paragrafo è il caricamento remoto sicuro di dati nella CIE da parte dell'Ente che eroga il servizio , questo processo è chiamato Secure Messaging.

I processi di Autenticazione e di Secure Messaging garantiscono l'interazione diretta tra Ente e Carta di Identità Elettronica e prevengono dai tentativi di intrusione che possono essere condotti sulla rete.

Il processo di autenticazione esterna utilizza metodologie di crittografia asimmetrica tramite la chiave pubblica del servizio(S_{pub}) mentre il processo di secure messaging utilizza crittografia simmetrica.

Per quanto concerne la gestione delle chiavi simmetriche sono stati oggetto di valutazione i seguenti due metodi :

- quello basato sullo utilizzo di *"diversified key"* (K_s) derivate da *"master key"*(K_m) e caricate nella CIE durante la fase di Installazione dei servizi;
- quello basato sullo scambio di una chiave di sessione (K_s) generata in modo casuale dalla CIE e crittografata ed autenticata dalla CIE stessa.

Il primo metodo è consolidato e comunemente impiegato nelle applicazioni *"Smart Card Based"* ma richiede particolare attenzione nella custodia e distribuzione delle chiavi.

Il secondo metodo, in fase di valutazione, richiede la scrittura di un comando ad hoc che consente la generazione, la crittografia e la autenticazione della chiave di sessione all'interno della CIE al fine di garantire alla Applicazione Server che quella chiave può essere decrittografata solo da lei e generata solamente dalla CIE.

6.7 Autenticazione esterna

Il processo di autenticazione esterna è attivato dall'applicazione remota che deve poter accedere ai file della Carta di Identità Elettronica per aggiornarne i dati.

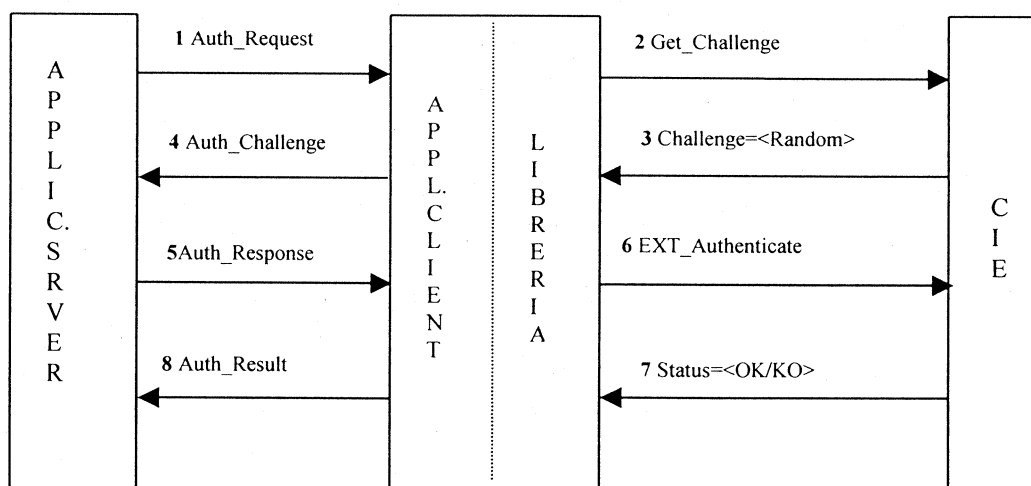
Questo processo utilizza la chiave pubblica del servizio(S_{pub}) che è stata caricata nella carta durante la fase di installazione del servizio.

L'Autenticazione Esterna coinvolge i seguenti moduli:

- applicazione Server
- applicazione Client
- libreria di interfaccia e CIE.

La Figura [5] schematizza un esempio di flusso di informazioni scambiate tra i vari moduli che concorrono al processo di autenticazione esterna.

Il processo di Autenticazione Esterna è attivato dalla applicazione Server dopo che è stata riconosciuta (autenticata) la Carta ed il titolare.

Figura [5]

Orientativamente, il processo di Autenticazione si svolge secondo i seguenti passi procedurali:

1. L'Applicazione Server richiede alla Applicazione Client di essere autenticata dalla CIE (ad es. tramite il comando "**Aut_Request**");

2. L'applicazione Client, servendosi della LIBRERIA , invia una "challenge" alla CIE (ad es. con il comando "**Get_Challenge**");

3. La risposta della CIE è un numero random (il Challenge);

4. L'Applicazione Client invia alla Applicazione Server il numero random generato dalla CIE (ad es. con il comando "**Aut_Challenge**");

5. L'Applicazione Server firma il Challenge con la chiave privata del servizio(S_{pri}), e lo invia alla Applicazione Client (ad es. con il comando "**Auth_Response**");

6. La applicazione Client, servendosi della libreria, richiede alla CIE un'operazione di "autenticazione esterna";

7. La CIE utilizza la chiave pubblica del servizio(S_{pub}) , relativa alla directory a cui si vuole accedere, per verificare la autenticità del Response; se la verifica è positiva viene inviato un messaggio di consenso alla Applicazione Client tramite la libreria e viene reso disponibile l'accesso ai file appartenenti a quella directory;

8. L'Applicazione Client comunica alla Applicazione Server l'esito del processo (ad es. tramite il messaggio "Auth_Result");

Nella descrizione del processo di Autenticazione Esterna si sono trascurati dettagli procedurali quali la gestione delle eventuali anomalie e le "Retry" tipiche di questi processi in quanto non incidono sulle funzionalità della CIE.

6.8 Secure Messaging

Il processo di Secure Messaging è attivato dopo i processi di autenticazione e consente lo scambio dati crittografato tra CIE ed Applicazione Server .

Esso utilizza una chiave di sessione diversificata $\mathbf{K_D}$ che è:

- derivata da $\mathbf{K_S}$ attraverso la generazione di una quantità Random, qualora venga scelto di distribuire le chiavi secondo metodi convenzionali durante la fase di emissione;

- coincidente con la chiave $\mathbf{K_S}$, autogenerata in modalità casuale, qualora venga scelta la distribuzione delle chiavi di sessione dalla CIE alle Applicazioni Server con un apposito comando basato sull'utilizzo di crittografia asimmetrica.

Il comando di Secure Messaging dovrà essere implementato secondo la norma ISO 7816-4 nella modalità "Secure Messaging for Confidentiality".

7. Processo di Emissione

Nel presente capitolo sono descritte in dettaglio le fasi operative previste dal circuito d'emissione. Per una migliore comprensione del processo d'emissione si riporta un glossario di riferimento.

Fb	**Fornitori Bande Ottiche**
Fp	**Fornitori microprocessori**
IPZS	**Istituto Poligrafico Zecca dello Stato**
SSCE	**Sistema di sicurezza del circuito di emissione** (Ministero dell'Interno)
E	**Ente emettitore della CIE, Tipicamente un comune.**
ID_Carta	**Numero identificativo della carta** Numero assegnato al documento d'identità e generato dal sistema di sicurezza.
C_Carta	**Certificato anticontraffazione della carta** - Certificato che lega il numero identificativo del documento ed una chiave pubblica (**Kpub**), corrispondente ad una privata (**Kpri**), generata all'interno del microprocessore e non esportabile all'esterno. - E' rilasciato dal SSCE e viene riportato nella banda ottica e nel microprocessore. - Unisce in maniera inscindibile i due supporti informatici.
Dati_processore	**E' un file elementare che riporta alcuni dati univoci del processore** Le informazioni che contiene sono:Fp, **numero seriale** e **data fabbricazione**.
Dati_banda_ottica	**E' un file elementare che riporta alcuni dati identificativi univoci della banda ottica** Le informazioni che contiene sono: Fb, **numero seriale** e **data fabbricazione**
Rd	**Record dati.** **E' un'area della banda ottica che contiene i dati necessari**
PIN P1	**Cifrato con la chiave pubblica del comune di destinazione. Serve per abilitare l'accesso in scrittura ai files elementari. Securizza ulteriormente la fase di compilazione.**
PIN utente	**E' il PIN necessario al titolare per utilizzare la chiave privata Kpri per le operazioni di autenticazione in rete. Viene consegnato dal comune di rilascio con meccanismi di sicurezza (es. busta in carta chimica protetta).**

7.1 Produzione di banda laser e microprocessore

I Fornitori di microprocessori (**Fp**) ed i Fornitori di bande ottiche (**Fb**) provvedono alla fabbricazione dei supporti informatici.

I Fornitori di microprocessori provvedono anche alla mascheratura in ROM del Sistema Operativo.

Entrambi i fornitori applicano, in fase di produzione, un numero seriale progressivo univoco, sui supporti informatici da loro forniti e predispongono una distinta, cartacea ed elettronica, che riporta le seguenti indicazioni: ID fornitore, numero seriale, numero del lotto di produzione, data di produzione.

I fornitori, successivamente, inviano i loro prodotti, accompagnati dalle distinte, direttamente all'Istituto Poligrafico dello Stato (IPZS).

7.2 Produzione ed inizializzazione della carta d'identita elettronica e del documento elettronico

Per meglio comprendere le diverse fasi del circuito di emissione, è bene fare dei brevi cenni sull'organizzazione e sulla normalizzazione delle informazioni sui supporti informatici della CIE.

7.2.1 Struttura delle informazioni sulla banda ottica

Sulla banda ottica vi sono due aree di memorizzazione differenti ma sincrone:

- Una **area dati** che contiene, codificati in record di formato opportuno (R_d), i necessari dati della carta, del titolare e i servizi installati.
- Una **area di controllo** che contiene, codificate in formato opportuno (R_c), le informazioni di controllo e verifica dei corrispondenti R_d.

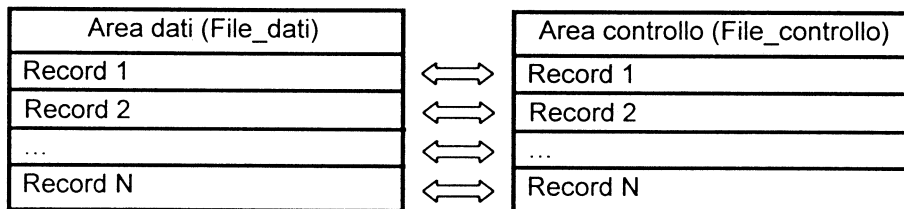
L'area controllo è assimilabile ad un registro incrementale delle operazioni avvenute sulla carta, e consente di stabilire con certezza *chi*, *dove* e *quando* ha effettuato ed autorizzato ogni operazione. La certezza viene stabilita dall'uso incrociato dei "sigilli" apposti da:

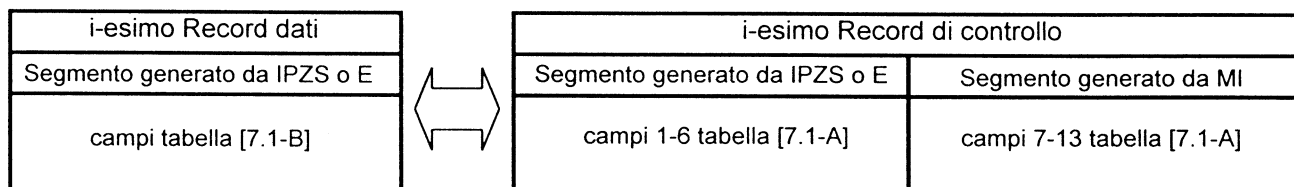
- Istituto Poligrafico dello Stato;
- comuni;
- SSCE.

A ciascun record R_d dell'area dati corrisponde un record R_c dell'area di controllo. I record dati possono avere formati multipli secondo necessità.

I record R_d dell'area dati sono formati da **IPZS** e da **E**. I record R_c dell'area di controllo sono composti da due parti: una formata da **IPZS** e da **E**, l'altra formata da **SSCE**.

La successiva figura mostra l'organizzazione in record corrispondenti dell'area dati (File_dati) e dell'area di controllo (File_controllo):

Area dati (File_dati)		Area controllo (File_controllo)
Record 1	⇔	Record 1
Record 2	⇔	Record 2
...	⇔	...
Record N	⇔	Record N

La successiva figura mostra, invece, per ciascun record corrispondente dell'area dati e di quella di controllo, la suddivisione in campi:

i-esimo Record dati		i-esimo Record di controllo	
Segmento generato da IPZS o E	⇔	Segmento generato da IPZS o E	Segmento generato da MI
campi tabella [7.1-B]		campi 1-6 tabella [7.1-A]	campi 7-13 tabella [7.1-A]

Questi record contengono dunque richieste (di IPZS o E) ed approvazioni (di SSCE), e permettono di far avanzare la carta da uno stato all'altro, lungo il "percorso" che la porta dalla manifattura fino al momento del rilascio al titolare.

Questo flusso di richiesta ed approvazione è lo stesso utilizzato anche per il microcircuito, per cui nel record di controllo sono presenti elementi che andranno poi memorizzati nel chip (come il certificato C_Carta), e che consentono in tal modo anche un utile corrispondenza dei dati tra chip e banda ottica.

La tabella seguente definisce la struttura (campi) del record di controllo:

Campo	*Generato da*	*Descrizione*	*Note*
1	IPZS, E (S)	Numero progressivo del record nell'ambito della carta	Questa informazione è sempre presente
2	IPZS, E (S)	Tipo del record (ossia dell'operazione)	Inizializzazione o Emissione
3	IPZS, E (S)	Data e ora della creazione del record	Questa informazione è sempre presente
4	IPZS, E (S)	Certificato dell'ente che ha creato il record	Questa informazione è sempre presente. Il certificato è emesso da MI.
5	IPZS, E (S)	Identificativo dell'operatore che ha creato il record	Questa informazione ordinariamente è sempre presente, salvo casi eccezionali in cui non sia previsto l'intervento manuale di un operatore nella generazione del record.

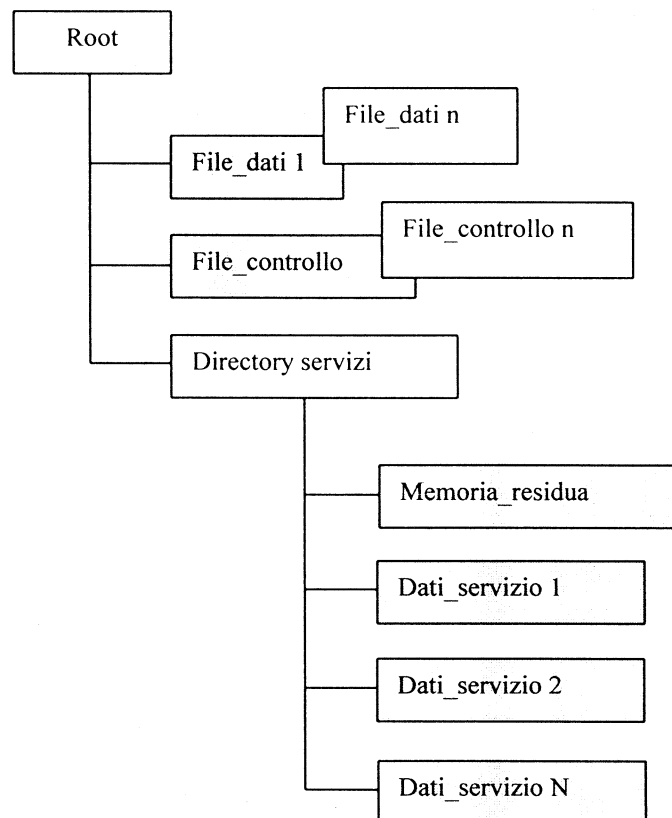
6	IPZS (F_c), E (S)	Bollo elettronico dell'ente che ha creato il record.	Coincide con la firma del record dati (R_d) e dei campi [1-5] del corrispondente record di controllo (R_c), utilizzando la chiave relativa al certificato (4). Il bollo elettronico certifica i dati generati dall'ente che li ha generati ed immessi nel circuito.
7	SSCE	Numero progressivo dell'autorizzazione concessa (generato secondo un protocollo interno di SSCE)	Questa informazione è sempre presente.
8	SSCE	Data ed ora dell'autorizzazione	Questa informazione è sempre presente.
9	SSCE	Numero identificativo della carta	è il numero (ID_Carta) assegnato al documento d'identità da SSCE e stampato anche sul supporto plastico.
10	SSCE	Certificato del SSCE	Questa informazione è sempre presente.
11	SSCE	Identificativo dell'operatore che ha creato il record	Questa informazione ordinariamente è assente, salvo casi eccezionali in cui sia previsto l'intervento manuale di un operatore nella generazione del record (ad es. se durante i controlli automatici emergono condizioni per cui è necessaria un'indagine più approfondita su un determinato individuo, ecc.).
12	SSCE	Certificato anti-contraffazione della carta	E' il certificato (C_Carta) che lega il numero identificativo della carta (ID_Carta) ed una chiave pubblica (K_{pub}), corrispondente ad un'unica chiave privata (Kpri), generata all'interno del microcircuito e non esportabile all'esterno di esso. Esso è rilasciato da SSCE per essere memorizzato oltre che sulla banda ottica, anche nel microcircuito. Questa informazione permette di legare in modo biunivoco il microcircuito e la banda ottica presenti sulla stessa carta.
13	SSCE	Bollo elettronico dell'ente di controllo e verifica.	Coincide con la firma del record dati (R_d) e dei campi [1-12] del corrispondente record di controllo (R_c), utilizzando la chiave relativa al certificato (10). Il bollo elettronico certifica l'approvazione, da parte dell'ente di controllo e verifica, dei dati di inizializzazione e/o personalizzazione della carta.

La seguente tabella definisce la struttura (campi) del record dati.

Campo	*Generato da*	*Descrizione*	*Note*
1	IPZS, E	Numero progressivo del record nell'ambito dell'area dati (File_dati). Il numero progressivo di ogni record dell'area dati deve corrispondere a quello del record dell'area di controllo che descrive l'operazione eseguita per generarlo e contiene le relative approvazioni (firme)	Questa informazione è sempre presente
2	E	Embedded Hologram.	Viene "impresso" anche in evidenza visiva sulla banda ottica al momento dell'emissione. Solo il record che descrive questa fase è non nullo.
3	IPZS	Dati identificativi univoci della banda ottica (n. serie, lotto di produzione, fabbricante, ecc.)	Non nullo solo nel record relativo all'inizializzazione, eseguita da IPZS. Questi dati vengono comunicati dai fornitori della banda ottica
4	E	Chiave biometrica individuale.	Non nullo solo nel record relativo all'emissione, eseguita dal comune.
5	E	Dati personali dell'individuo, con l'eccezione della fotografia.	Non nullo solo nel record relativo all'emissione, eseguita dal comune.
6	E	Fotografia.	Non nullo solo nel record relativo all'emissione, eseguita dal comune.

La successiva figura descrive la struttura di memorizzazione della banda ottica. Le due aree di memorizzazione denominate File_dati e File_controllo sono state già descritte in precedenza.

Una directory servizi è predisposta ad accogliere le strutture di memorizzazione relative ad eventuali servizi (Dati_servizo 1, 2,..., N), che avessero necessità di appoggiarsi a grosse aree di memorizzazione off-line, disponibili sulla banda ottica.

Il file Memoria_residua mantiene lo stato attuale della memoria, che decresce sempre, essendo la banda ottica un supporto non riscrivibile.

7.2.2 Struttura delle informazioni nel microprocessore

La successiva tabella definisce la struttura dei dati registrati nella memoria riscrivibile (EEPROM) del microcircuito.

Fornito da: indica l'operazione in ragione della quale viene messo a disposizione un contenuto informativo, consistente in una sequenza di *bytes*. Ad esempio, il risultato della raccolta dei dati personali del titolare, effettuata dall'ente emettitore (il comune).

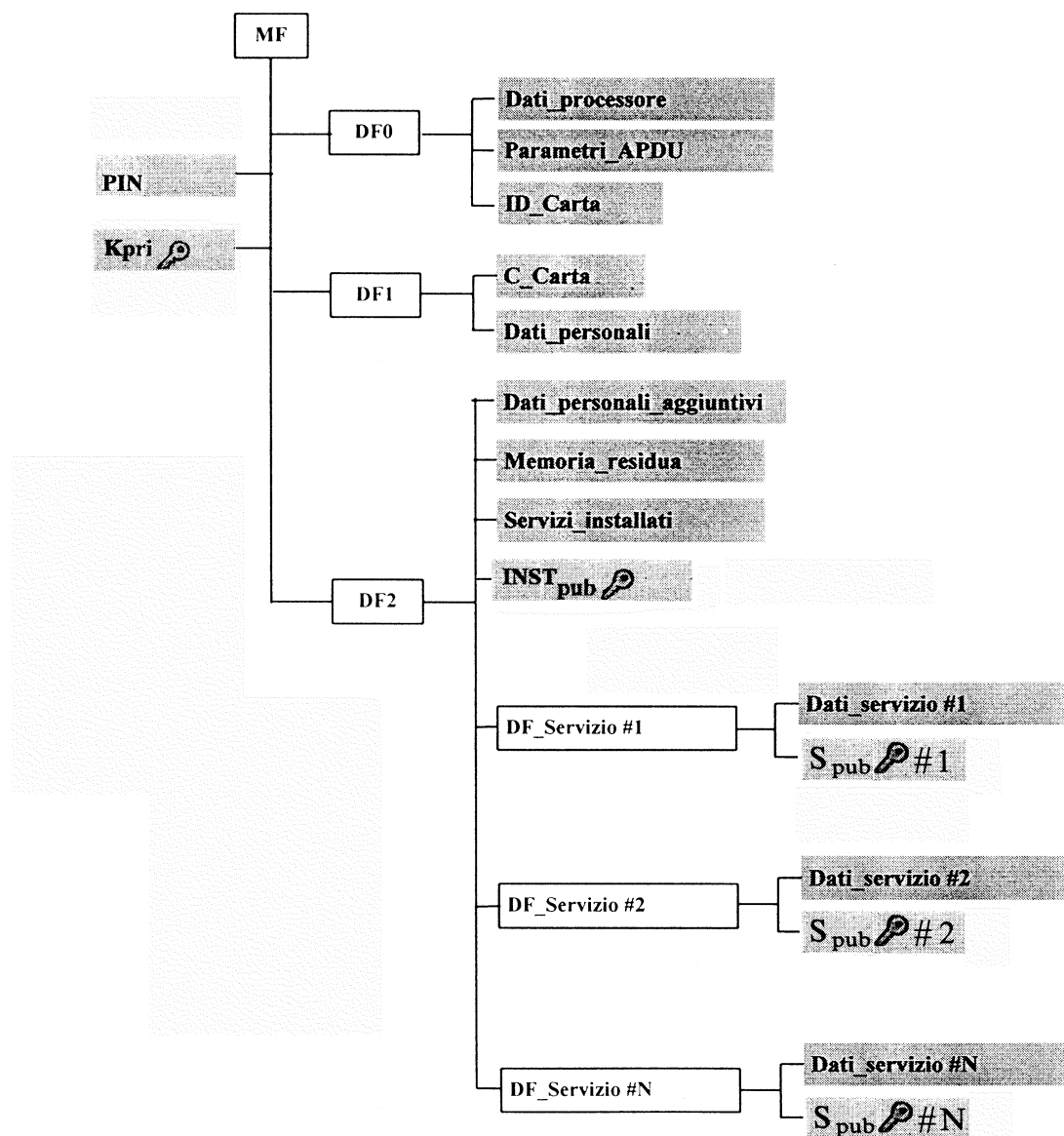
Predisposto da: indica l'operazione di creazione di una nuova struttura dati (DF o EF), ossia di un "contenitore" vuoto, pronto ad essere riempito con le informazioni che risultano da un'operazione del tipo precedente.

Scritto da: è l'operazione con la quale un contenitore vuoto (EF) viene riempito con le informazioni che risultano da una precedente operazione di generazione.

#	*Elemento*	*Fornito da*	*Predisposto*	*Scritto da*	*Descrizione*
1	MF		IPZS		E' il "Master File" della struttura di memorizzazione. Corrisponde più o meno alla directory radice di un ordinario sistema operativo.
2	DF0		IPZS		Dedicated file (directory) dove vengono memorizzate le informazioni prodotte durante la fase di inizializzazione della carta.
3	DF1		IPZS		Dedicated file (directory) dove vengono memorizzate le informazioni raccolte durante la fase di personalizzazione della carta.
4	DF2		IPZS		Dedicated file (directory) dove vengono installati i servizi che necessitano, per il loro funzionamento, di una struttura dati riservata nella memoria riscrivibile (EEPROM) del microcircuito.
5	PIN	E	E	E	E' il PIN utente richiesto per usare la chiave privata K_{pri} per le operazioni di autenticazione. Questo codice deve essere consegnato dal comune di rilascio, con garanzia di

					segretezza, al titolare della CIE.
6	K_{pri}		E		Chiave autogenerata internamente alla carta, congiuntamente a K_{pub}. Essa è invisibile all'esterno, ma utilizzabile per le operazioni di cifra richieste durante l'operazione di strong authentication. Il microcircuito deve essere provvisto di un motore crittografico interno (crypto-engine), al fine di rendere più rapide tali operazioni.
7	$INST_{pub}$	E	IPZS	IPZS	Chiave pubblica del servizio di installazione delle strutture dati relative ai servizi. La responsabilità operativa del processo di installazione del servizio è delegata ai comuni.
8	Dati_processore	IPZS	IPZS	IPZS	E' un file elementare (EF) che riporta alcuni dati identificativi univoci del processore (n. serie, lotto di produzione, fabbricante, ecc.)
9	Parametri_APDU	F_p	IPZS	IPZS	E' un file elementare che riporta le particolarità dei comandi elementari (APDU) del sistema operativo della carta, al fine di rendere interoperabili le applicazioni.
10	ID_Carta	SSCE	IPZS	IPZS	Numero identificativo (matricola) della carta d'identità, generato dal Ministero dell'Interno e corrispondente al numero stampato da IPZS sul supporto plastico.
11	C_Carta	SSCE	IPZS	E	E' il certificato, rilasciato da SSCE, che garantisce la validità del legame tra la componente pubblica, K_{pub}, della coppia di chiavi generata internamente al microcircuito, e ID_Carta; esso contiene, come estensione, il risultato dell'esecuzione di una funzione di hash sui dati identificativi

					raccolti all'atto della formazione della carta (e riportati anche sul supporto plastico).
12	Dati_personali	E	IPZS	E	E' un file elementare che contiene i dati personali dell'individuo, con l'eccezione della fotografia.
13	Dati_personali aggiuntivi	E	IPZS	E	E' un file elementare che contiene dati, relativi alla persona, che integrano le informazioni anagrafiche, che possono essere necessarie ai fini dell'erogazione di alcuni servizi.
14	Memoria_residua	E	IPZS	E	E' l'ammontare dello spazio totale previsto per i servizi, decurtato dello spazio utilizzato da quelli già installati.
15	Servizi_installati	E	IPZS	E	E' un file elementare che riporta l'elenco dei servizi già installati sulla carta.
16	DF_Servizio #1, DF_Servizio #2, ... DF_Servizio #N	E	E	E	Sono le strutture dati relative ai servizi installati sulla carta. Esse comprendono, quando il servizio richiede particolari garanzie di sicurezza, la chiave pubblica del servizio per l'autenticazione in rete di quest'ultimo da parte della carta (S_{pub}).

La successiva figura descrive graficamente la struttura di memorizzazione interna al microprocessore:

7.3 Le fasi preliminari

L'Istituto Poligrafico, responsabile della manifattura della CIE, riceve dalle Prefetture, in via telematica, le richieste di fornitura di "documenti in bianco", distinte per Comune, e dai fornitori i microprocessori e le bande ottiche.

La consegna, alle Prefetture, dei "documenti in bianco" avviene al termine delle seguenti sottofasi di generazione numeri identificativi, produzione, inizializzazione ed incisione grafica degli elementi costanti.

7.3.1 Generazione numeri identificativi per le carte d'identità ed i documenti elettronici.

L'IPZS richiede al SSCE i numeri identificativi (ID_Carta) necessari;
SSCE genera i nuovi ID_Carta ed inserisce un equivalente numero di record "in attesa"di divenire CIE nel suo database centrale;
L'IPZS riceve via telematica i lotti di numeri identificativi da assegnare alle nuove carte in corso di produzione.

7.3.2 Produzione

L'IPZS, attiva le procedure necessarie ai fini della:

- predisposizione del supporto fisico;
- inserimento nel supporto fisico della pellicola di banda ottica e del microprocessore;
- stampa del logo e degli elementi grafici costanti e di sicurezza;
- inizializzazione elettrica del microprocessore.

7.3.3 Inizializzazione

La sottofase di inizializzazione, una delle più delicate dell'intero processo di emissione, consente di trasformare i tre supporti previsti, in un unico elemento inscindibile.

Dopo la fase di integrazione fisica del supporto plastico, con la banda ottica ed il microprocessore, l'inizializzazione provvede alla integrazione logica tramite l'apposizione di codici univoci.

Mentre risulta di immediata applicazione il codice apposto graficamente sul supporto fisico, l'inizializzazione di quelli informatici ha quale prerequisito la loro "formattazione" che, di fatto, consiste nella loro strutturazione in "directory" e l'impostazione delle condizioni di test necessarie a definire i diritti di accesso alle directory.

Le directory, definite in dettaglio nei precedenti paragrafi, servono per tracciare tutte le fasi di inizializzazione e personalizzazione della Carta, per consentire l'installazione dei servizi qualificati e per normalizzare i dati identificativi del titolare, le informazioni alfanumeriche nonchè le immagini.

In particolare, IPZS provvede alla:

- generazione della struttura dati interna della banda ottica;
- generazione della struttura dati interna del microprocessore;
- scrittura dei files elementari che riportano i dati specifici del microprocessore ("Dati_processore), della banda ottica ("Dati_banda_ottica") e del sistema operativo ("Parametri_APDU");
- scrittura ID_Carta;
- impostazione delle condizioni di accesso a tali file;
- scrittura del record dati (Rd) e di alcuni campi (1-6) di quello di controllo (Rc) relativi all'operazione di inizializzazione. Il record di controllo deve contenere almeno:
  - ID_Carta;
  - Dati_Processore / Dati_Banda_Ottica;
  - Data di fabbricazione;
  - PIN P1 (per abilitare l'accesso in scrittura dei files elementari che devono essere riempiti dal Comune al momento della formazione della carta) cifrato con la chiave pubblica del comune).
  - Indicazione della Provincia e del comune cui la carta e' destinata.
- inserimento del record dati e di quello di controllo in coda ad un file di richieste di autorizzazione da inviare a SSCE;
- stampa dello sfondo, del Logo, del numero di carta (ID_Carta, quello generato da SSCE) e degli altri elementi costanti;
- incisione grafica sulla banda ottica (Embedded Hologram) degli elementi costanti e dell'ID_Carta;
- stoccaggio della carta.

7.3.4 Attivazione

Al termine della presente sottofase la carta d'identità risulta "attivata", e diventa "documento in bianco", ossia pronto alla fase successiva di formazione e rilascio, ad opera dei Comuni.

Durante la presente sottofase l'IPZS esegue le seguenti attività:

- riceve da SSCE il file di approvazione per attivare il lotto di carte in lavorazione;
- inserisce le carte, che fanno parte del lotto autorizzato, nello/negli apparati per la lettura del chip e della banda ottica e legge l'ID_Carta contenuto nei due supporti (la lettura in entrambi i supporti costituisce un ulteriore controllo sui dati inseriti);
- trasmette a SSCE le associazioni ID_Carta/Provincia richiedente;
- invia le carte in bianco attivate alle Prefetture. Queste ultime sono, a loro volta, incaricate della distribuzione nella provincia di loro competenza agli enti autorizzati alle procedure di emissione (Comuni E).

Al completamento di questa fase il data base di SSCE conterrà tanti record quante sono le carte in bianco in attesa di formazione. Tali record contengono già informazioni come il numero identificativo della carta (ID_Carta), la Provincia ed il Comune di destinazione.

Durante la fase di personalizzazione i campi di tali record verranno ulteriormente popolati con i codici fiscali (scritti in chiaro) dei titolari e con i dati identificativi (scritti in forma cifrata) degli stessi.

La cifratura avverrà, tramite un sistema automatico, utilizzando la chiave pubblica della Questura, territorialmente competente, e quella del comune che ha rilasciato la Carta d'Identità Elettronica.

7.4 Personalizzazione ed emissione delle carte

La formazione delle carte ed il loro rilascio è condotta direttamente dai Comuni .
Nei paragrafi successivi le chiavi asimmetriche saranno indicate con la seguente notazione:

- $K_{pri-aut}$, chiave privata di autenticazione;
- $K_{pub-aut}$, chiave pubblica di autenticazione;
- $K_{pri-enc}$, chiave privata di crittografia;
- $K_{pub-enc}$, chiave pubblica di crittografia.

7.4.1 Ricezione dei documenti in bianco (fa riferimento all'art. 12 del D.M.)

- Il comune, per il tramite delle Prefetture della propria provincia, riceve i documenti in bianco;
- I documenti devono essere conservati dai comuni in appositi armadi di sicurezza, possibilmente in locali ad accesso riservato.

7.4.1.1 Sottofase di Compilazione

- Il Comune riceve i "documenti in bianco" da parte della Prefettura;
- tramite il software di sicurezza, le informazioni del titolare sono riportate dal comune nel sistema. I dati sono quelli indicati in dettaglio al paragrafo 4.4.
  La fotografia può essere catturata direttamente, tramite videocamera digitale o digitalizzata per mezzo di uno scanner.
  Anche per digitalizzare la firma del titolare può essere utilizzato uno scanner oppure può essere catturata direttamente tramite tavoletta grafica.
  Per l'impronta digitale, laddove il comune decida di assumerla o il richiedente desideri inserirla nella propria CIE, e' necessario utilizzare un lettore di impronte digitali (live scan);
- Generazione della coppia di chiavi K_{pri} e K_{pub} (della carta) necessarie per garantire l'autenticazione in rete della carta e generazione del relativo PIN utente. La generazione di queste chiavi avviene all'interno del microprocessore.
- Cifratura simmetrica dei dati a 128 bit. La cifratura viene eseguita automaticamente dal software di sicurezza. La cifratura e' indispensabile per proteggere i dati durante la trasmissione al SSCE utilizzando la $K_{pub-enc}$ del SSCE stesso con una chiave di trasporto da 128 bit generata in maniera dinamica sessione per sessione;
- Apposizione del bollo elettronico del comune, per mezzo della $K_{pri-aut}$ (Comune). L'apposizione di tale bollo garantisce il mittente al SSCE;
- Invio della richiesta di emissione carta d'identità al SSCE per via telematica

7.4.1.2 Sottofase di autorizzazione

La sottofase di autorizzazione viene effettuata dal SSCE quando, da un qualsiasi comune, riceve una richiesta di rilascio di una nuova CIE . Vengono eseguite le seguenti attività:

1) **SSCE** riceve i dati raccolti dal comune;
2) **SSCE** estrae, tramite la la propria $K_{pri\text{-}enc}$, il record dati;
3) **SSCE** mantiene in chiaro codice fiscale, provincia e comune richiedente e cifra tutte le altre informazioni con due chiavi: la $K_{pub\text{-}aut}$ del comune richiedente e la $K_{pub\text{-}aut}$ della Questura territorialmente competente;
4) **SSCE** esegue il controllo automatico di "non esistenza" sulla propria base dati, tramite i dati in chiaro e la K_{pub} della CIE;
   a) Controllo positivo (es. CIE già rilasciata per quel codice fiscale, richiesta avanzata da un comune diverso da quello previsto e soprattutto che la K_{pub} della CIE non sia identica ad una già certificata, etc.) viene rigettata la richiesta non vengono seguite ulteriori attività e all'ente emettitore viene ritornato un opportuno codice di errore .
   b) Controllo negativo (la richiesta può essere soddisfatta) .
5) **SSCE** trasmette l'esito dell'operazione di autorizzazione. I dati vengono inviati cifrati utilizzando la $K_{pub\text{-}enc}$ del Comune ed una chiave di trasporto a 128 bit generata sessione per sessione e certificati con il bollo elettronico del SSCE ($K_{pri\text{-}aut}$ di SSCE).

7.4.1.3 Sottofase di formazione

Sottofase di competenza dell'Ente emettitore che riporta i dati su tutti i supporti: microprocessore, banda ottica e grafici sul supporto fisico. La criticità maggiore sta nel fatto che, qualsiasi inconveniente possa verificarsi non deve mettere a rischio l'integrità dei dati (per es. scrivendo infomazioni diverse sui vari supporti). Allo scopo si suggerisce di garantire agli strumenti informatici continuità elettrica.

1) **E** riceve il record dati validato da SSCE;
2) memorizza i dati nel microprocessore;
3) memorizza i dati nella banda ottica. Al fine di garantire l'allineamento delle informazioni il lettore/scrittore di banda ottica dovrebbe avere la possibilità di leggere anche il microprocessore. Al fine di consentire una identificazione sicura, e dare certezza sulla originalità della CIE, i dati memorizzati nella banda ottica devono essere quelli firmati con il bollo elettronico del SSCE.
4) stampa grafica dei dati sul supporto fisico. Anche in questo caso sarebbe opportuno che la stampante sia in grado di leggere il microprocessore.
5) stampa del PIN utente su speciale carta chimica retinata, tale da garantire la riservatezza dell'informazione contenuta e di evidenziare eventuali tentativi di apertura.

7.4.1.4 Sottofase di rilascio

Anche questa sottofase e' di esclusiva competenza dei comuni che:

1) rilasciano la CIE al cittadino che ne ha fatto richiesta;
2) consegnano la busta contenente il PIN utente;
3) comunicano a SSCE l'avvenuto rilascio tramite comunicazione telematica diretta.

7.4.1.5 Sottofase di verifica e controllo

La verifica ed il controllo sono le uniche attività sempre presenti in tutte le sottofasi di lavorazione della CIE, dal momento della produzione fino al loro rilascio e vengono condotte da SSCE. Per questo motivo tutti gli enti coinvolti nei vari momenti del processo devono disporre di una connessione telematica con il Sistema.

Ovviamente la verifica ed il controllo citato nel processo di formazione, non è riferito a quello che verrà dettagliato nel capitolo successivo che, invece, si riferisce ai controlli effettuabili dalla Polizia come previsto dal Testo Unico delle Leggi di P.S.

8. Verifica delle carte di identità elettroniche (fa riferimento all'art. 6, comma 1 del D.M.)

Nel presente capitolo sono descritti in dettaglio i casi in cui è consentito l'accesso alle CIE ed alle informazioni in esse contenute. Vengono, altresì, indicati gli organi competenti e le modalità di accesso.

8.1 Conservazione del cartellino elettronico (fa riferimento all'art. 6, comma 3 del D.M.)

Il processo di ammodernamento della CIE deve necessariamente portare ad una differente interpretazione di alcune delle norme precedenti, soprattutto di quelle destinate alla gestione del modello cartaceo, ormai superato.

E' pressoché intuitivo come non trovino ragione di essere le prescrizioni relative alla conservazione e consultazione della copia del cartellino presente in ciascuna Questura. L'obbligo previsto per i Comuni di trasmettere copia del cartellino per ogni carta di identità rilasciata, viene sostituito dalla seguente procedura prevista per il nuovo cartellino elettronico:

- i Comuni eseguono le attività di formazione e rilascio delle CIE;
- SSCE riceve comunicazione che è stata rilasciata la CIE e memorizza la copia elettronica, della stessa, nell'archivio della Questura territorialmente competente. La copia elettronica, viene cifrata con la chiave pubblica della Questura stessa. Tale modalità consente di attendere al Testo Unico delle Leggi di P.S. che indica nelle Questura l'ufficio a cui è demandata la conservazione della copia delle CIE;
- i controlli sulle CIE, una volta memorizzate, possono essere effettuati secondo le seguenti modalità:
  - da qualsiasi operatore delle Forze di Polizia tramite controlli a vista, apparecchiature stand-alone (lettori di banda ottica) o transazioni a SSCE. In quest'ultimo caso, se la richiesta arriva da una Questura di una Provincia diversa da quella dove è stato rilasciata la CIE, l'operatore può, tramite il codice fiscale del titolare o il numero della CIE verificarne l'esistenza, il comune e la provincia in cui è stata rilasciata, non può vedere nel dettaglio le informazioni della CIE;
  - da un operatore della Questura nella cui Provincia è stata rilasciata la CIE. In questo caso l'operatore può, tramite il codice fiscale del titolare o il numero di CIE, verificarne l'esistenza e, tramite l'inserimento della propria chiave privata, verificarne anche il contenuto nel dettaglio.
- le Questure territorialmente competenti tramite SSCE conservano e consultano la copia elettronica della CIE. Possono eseguire anche stampe e tutte le attività già possibili con la passata gestione.

8.2 Interdizione dell'operatività della CIE (fa riferimento all'art. 6, comma 2 del D.M.)

Le carttarestiche principali della nuova CIE, che la differenziano dal vecchio modello cartaceo, sono rappresentate dalla presenza dei supporti informatici e dalla gestione centralizzata del flusso di

emissione. Entrambi gli elementi da un lato aumentano il livello di sicurezza del nuovo documento e dall'altro offrono la possibilità di accesso a servizi telematicisia nazionali che locali.

Proprio questa nuova possibilità di accedere a servizi implica la necessità di dover interdire, più che in passato, l'utilizzo della CIE che potrebbe essere impiegata, in caso di furto o smarrimento, da persone diverse dal titolare.

Nel seguito vengono descritte le modalità a cui è necessario attenersi in caso di furto o smarrimento di una CIE.

- il titolare telefona al numero verde e comunica l'avvenuto smarrimento/furto della CIE;
- per motivi di sicurezza, l'interdizione temporanea della CIE avviene dopo che è stata svolta una successiva verifica telefonica;
- a seguito di tale comunicazione nel record relativo alla CIE viene apposto un "flag" e, per un periodo di 7 (sette) gg, la CIE non è in grado di accedere a servizi;
- successivamente alla comunicazione telefonica, il titolare della CIE deve presentare regolare denuncia ad un ufficio di Polizia;
- la denuncia viene trasmessa alla Questura della Provincia dove è stata rilasciata la CIE;
- la Questura inibisce, definitivamente, l'utilizzo in rete della CIE ed il titolare può richiedere un duplicato, recandosi al comune;
- se durante i sette gg. di interdizione momentanea non viene applicata l'interdizione definitiva, la CIE torna ad essere, nuovamente, "NON interdetta".

00A10094

DOMENICO CORTESANI, *direttore*

FRANCESCO NOCITA, *redattore*
ALFONSO ANDRIANI, *vice redattore*

(3651434/1) Roma, 2001 - Istituto Poligrafico e Zecca dello Stato - S.

ISTITUTO POLIGRAFICO E ZECCA DELLO STATO

LIBRERIE CONCESSIONARIE PRESSO LE QUALI È IN VENDITA LA GAZZETTA UFFICIALE

ABRUZZO

◇ **CHIETI**
LIBRERIA PIROLA MAGGIOLI - DE LUCA
Via A. Herio, 21

◇ **L'AQUILA**
LIBRERIA LA LUNA
Viale Persichetti, 9/A

◇ **PESCARA**
LIBRERIA COSTANTINI DIDATTICA
Corso V. Emanuele, 146
LIBRERIA DELL'UNIVERSITÀ
Via Galilei (ang. via Gramsci)

◇ **SULMONA**
LIBRERIA UFFICIO IN
Circonv. Occidentale, 10

◇ **TERAMO**
LIBRERIA DE LUCA
Via Riccitelli, 6

BASILICATA

◇ **MATERA**
LIBRERIA MONTEMURRO
Via delle Beccherie, 69
GULLIVER LIBRERIE
Via del Corso, 32

◇ **POTENZA**
LIBRERIA PAGGI ROSA
Via Pretoria

CALABRIA

◇ **CATANZARO**
LIBRERIA NISTICÒ
Via A. Daniele, 27

◇ **COSENZA**
LIBRERIA DOMUS
Via Monte Santo, 70/A

◇ **PALMI**
LIBRERIA IL TEMPERINO
Via Roma, 31

◇ **REGGIO CALABRIA**
LIBRERIA L'UFFICIO
Via B. Buozzi, 23/A/B/C

◇ **VIBO VALENTIA**
LIBRERIA AZZURRA
Corso V. Emanuele III

CAMPANIA

◇ **ANGRI**
CARTOLIBRERIA AMATO
Via dei Goti, 11

◇ **AVELLINO**
LIBRERIA GUIDA 3
Via Vasto, 15
LIBRERIA PIROLA MAGGIOLI
Via Matteotti, 30-32
CARTOLIBRERIA CESA
Via G. Nappi, 47

◇ **BENEVENTO**
LIBRERIA LA GIUDIZIARIA
Via F. Paga, 11
LIBRERIA MASONE
Viale Rettori, 71

◇ **CASERTA**
LIBRERIA GUIDA 3
Via Caduti sul Lavoro, 29-33

◇ **CASTELLAMMARE DI STABIA**
LINEA SCUOLA
Via Raiola, 69/D

◇ **CAVA DEI TIRRENI**
LIBRERIA RONDINELLA
Corso Umberto I, 253

◇ **ISCHIA PORTO**
LIBRERIA GUIDA 3
Via Sogliuzzo

◇ **NAPOLI**
LIBRERIA LEGISLATIVA MAJOLO
Via Caravita, 30
LIBRERIA GUIDA 1
Via Portalba, 20-23
LIBRERIA L'ATENEO
Viale Augusto, 168-170
LIBRERIA GUIDA 2
Via Merliani, 118
LIBRERIA I.B.S.
Salita del Casale, 18

◇ **NOCERA INFERIORE**
LIBRERIA LEGISLATIVA CRISCUOLO
Via Fava, 51;

◇ **NOLA**
LIBRERIA EDITRICE LA RICERCA
Via Fonseca, 59

◇ **POLLA**
CARTOLIBRERIA GM
Via Crispi

◇ **SALERNO**
LIBRERIA GUIDA
Corso Garibaldi, 142

EMILIA-ROMAGNA

◇ **BOLOGNA**
LIBRERIA GIURIDICA CERUTI
Piazza Tribunali, 5/F
LIBRERIA PIROLA MAGGIOLI
Via Castiglione, 1/C
GIURIDICA EDINFORM
Via delle Scuole, 38

◇ **CARPI**
LIBRERIA BULGARELLI
Corso S. Cabassi, 15

◇ **CESENA**
LIBRERIA BETTINI
Via Vescovado, 5

◇ **FERRARA**
LIBRERIA PASELLO
Via Canonica, 16-18

◇ **FORLÌ**
LIBRERIA CAPPELLI
Via Lazzaretto, 51
LIBRERIA MODERNA
Corso A. Diaz, 12

◇ **MODENA**
LIBRERIA GOLIARDICA
Via Berengario, 60

◇ **PARMA**
LIBRERIA PIROLA PARMA
Via Farini, 34/D

◇ **PIACENZA**
NUOVA TIPOGRAFIA DEL MAINO
Via Quattro Novembre, 160

◇ **RAVENNA**
LIBRERIA GIURIDICA DI FERMANI MAURIZIO
Via Corrado Ricci, 12

◇ **REGGIO EMILIA**
LIBRERIA MODERNA
Via Farini, 1/M

◇ **RIMINI**
LIBRERIA DEL PROFESSIONISTA
Via XXII Giugno, 3

FRIULI-VENEZIA GIULIA

◇ **GORIZIA**
CARTOLIBRERIA ANTONINI
Via Mazzini, 16

◇ **PORDENONE**
LIBRERIA MINERVA
Piazzale XX Settembre, 22/A

◇ **TRIESTE**
LIBRERIA TERGESTE
Piazza Borsa, 15 (gall. Tergesteo)

◇ **UDINE**
LIBRERIA BENEDETTI
Via Mercatovecchio, 13
LIBRERIA TARANTOLA
Via Vittorio Veneto, 20

LAZIO

◇ **FROSINONE**
LIBRERIA EDICOLA CARINCI
Piazza Madonna della Neve, s.n.c.

◇ **LATINA**
LIBRERIA GIURIDICA LA FORENSE
Viale dello Statuto, 28-30

◇ **RIETI**
LIBRERIA LA CENTRALE
Piazza V. Emanuele, 8

◇ **ROMA**
LIBRERIA ECONOMICO GIURIDICA
Via S. Maria Maggiore, 121
LIBRERIA DE MIRANDA
Viale G. Cesare, 51/E-F-G
LIBRERIA EDITALIA
Via dei Prefetti, 16 (Piazza del Parlamento)
LIBRERIA LAURUS ROBUFFO
Via San Martino della Battaglia, 35
LIBRERIA L'UNIVERSITARIA
Viale Ippocrate, 99
LIBRERIA IL TRITONE
Via Tritone, 61/A
LIBRERIA MEDICHINI
Via Marcantonio Colonna, 68-70
LA CONTABILE
Via Tuscolana, 1027

◇ **SORA**
LIBRERIA PIROLA MAGGIOLI
Via Abruzzo, 4

◇ **TIVOLI**
LIBRERIA MANNELLI
Viale Mannelli, 10

◇ **VITERBO**
LIBRERIA ''AR''
Palazzo Uffici Finanziari - Loc. Pietrare
LIBRERIA DE SANTIS
Via Venezia Giulia, 5

LIGURIA

◇ **CHIAVARI**
CARTOLERIA GIORGINI
Piazza N.S. dell'Orto, 37-38

◇ **GENOVA**
LIBRERIA GIURIDICA DI A. TERENGHI & DARIO CERIOLI
Galleria E. Martino, 9

◇ **IMPERIA**
LIBRERIA PIROLA MAGGIOLI - DI VIALE
Viale Matteotti, 43/A-45

LOMBARDIA

◇ **BERGAMO**
LIBRERIA LORENZELLI
Via G. D'Alzano, 5

◇ **BRESCIA**
LIBRERIA QUERINIANA
Via Trieste, 13

◇ **BRESSO**
LIBRERIA CORRIDONI
Via Corridoni, 11

◇ **BUSTO ARSIZIO**
CARTOLIBRERIA CENTRALE BORAGNO
Via Milano, 4

◇ **COMO**
LIBRERIA GIURIDICA BERNASCONI
Via Mentana, 15

◇ **GALLARATE**
LIBRERIA PIROLA MAGGIOLI
Via Pulicelli, 1 (ang. p. risorgimento)
LIBRERIA TOP OFFICE
Via Torino, 8

◇ **LECCO**
LIBRERIA PIROLA - DI LAZZARINI
Corso Mart. Liberazione, 100/A

◇ **LIPOMO**
EDITRICE CESARE NANI
Via Statale Briantea, 79

◇ **LODI**
LA LIBRERIA S.a.s.
Via Defendente, 32

◇ **MANTOVA**
LIBRERIA ADAMO DI PELLEGRINI
Corso Umberto I, 32

◇ **MILANO**
LIBRERIA CONCESSIONARIA IPZS-CALABRESE
Galleria V. Emanuele II, 13-15
FOROBONAPARTE S.r.l.
Foro Bonaparte, 53

◇ **MONZA**
LIBRERIA DELL'ARENGARIO
Via Mapelli, 4

◇ **PAVIA**
LIBRERIA GALASSIA
Corso Mazzini, 28

◇ **SONDRIO**
LIBRERIA MAC
Via Caimi, 14

◇ **VARESE**
LIBRERIA PIROLA - DI MITRANO
Via Albuzzi, 8

Segue: **LIBRERIE CONCESSIONARIE PRESSO LE QUALI È IN VENDITA LA GAZZETTA UFFICIALE**

MARCHE

◇ **ANCONA**
LIBRERIA FOGOLA
Piazza Cavour, 4-5-6
◇ **ASCOLI PICENO**
LIBRERIA PROSPERI
Largo Crivelli, 8
◇ **MACERATA**
LIBRERIA UNIVERSITARIA
Via Don Minzoni, 6
◇ **PESARO**
LIBRERIA PROFESSIONALE MARCHIGIANA
Via Mameli, 34
◇ **S. BENEDETTO DEL TRONTO**
LA BIBLIOFILA
Via Ugo Bassi, 38

MOLISE

◇ **CAMPOBASSO**
LIBRERIA GIURIDICA DI.E.M.
Via Capriglione, 42-44
CENTRO LIBRARIO MOLISANO
Viale Manzoni, 81-83

PIEMONTE

◇ **ALBA**
CASA EDITRICE I.C.A.P.
Via Vittorio Emanuele, 19
◇ **ALESSANDRIA**
LIBRERIA INTERNAZIONALE BERTOLOTTI
Corso Roma, 122
◇ **BIELLA**
LIBRERIA GIOVANNACCI
Via Italia, 14
◇ **CUNEO**
CASA EDITRICE ICAP
Piazza dei Galimberti, 10
◇ **NOVARA**
EDIZIONI PIROLA E MODULISTICA
Via Costa, 32
◇ **TORINO**
CARTIERE MILIANI FABRIANO
Via Cavour, 17
◇ **VERBANIA**
LIBRERIA MARGAROLI
Corso Mameli, 55 - Intra
◇ **VERCELLI**
CARTOLIBRERIA COPPO
Via Galileo Ferraris, 70

PUGLIA

◇ **ALTAMURA**
LIBRERIA JOLLY CART
Corso V. Emanuele, 16
◇ **BARI**
CARTOLIBRERIA QUINTILIANO
Via Arcidiacono Giovanni, 9
LIBRERIA PALOMAR
Via P. Amedeo, 176/B
LIBRERIA LATERZA GIUSEPPE & FIGLI
Via Sparano, 134
LIBRERIA FRATELLI LATERZA
Via Crisanzio, 16
◇ **BRINDISI**
LIBRERIA PIAZZO
Corso Garibaldi, 38/A
◇ **CERIGNOLA**
LIBRERIA VASCIAVEO
Via Gubbio, 14
◇ **FOGGIA**
LIBRERIA PATIERNO
Via Dante, 21
◇ **LECCE**
LIBRERIA LECCE SPAZIO VIVO
Via Palmieri, 30
◇ **MANFREDONIA**
LIBRERIA IL PAPIRO
Corso Manfredi, 126
◇ **MOLFETTA**
LIBRERIA IL GHIGNO
Via Campanella, 24
◇ **TARANTO**
LIBRERIA FUMAROLA
Corso Italia, 229

SARDEGNA

◇ **CAGLIARI**
LIBRERIA F.LLI DESSÌ
Corso V. Emanuele, 30-32
◇ **ORISTANO**
LIBRERIA CANU
Corso Umberto I, 19
◇ **SASSARI**
LIBRERIA MESSAGGERIE SARDE
Piazza Castello, 11
LIBRERIA AKA
Via Roma, 42

SICILIA

◇ **ACIREALE**
LIBRERIA S.G.C. ESSEGICI S.a.s.
Via Caronda, 8-10
CARTOLIBRERIA BONANNO
Via Vittorio Emanuele, 194
◇ **AGRIGENTO**
TUTTO SHOPPING
Via Panoramica dei Templi, 17
◇ **CALTANISSETTA**
LIBRERIA SCIASCIA
Corso Umberto I, 111
◇ **CASTELVETRANO**
CARTOLIBRERIA MAROTTA & CALIA
Via Q. Sella, 106-108
◇ **CATANIA**
LIBRERIA LA PAGLIA
Via Etnea, 393
LIBRERIA ESSEGICI
Via F. Riso, 56
LIBRERIA RIOLO FRANCESCA
Via Vittorio Emanuele, 137
◇ **GIARRE**
LIBRERIA LA SENORITA
Corso Italia, 132-134
◇ **MESSINA**
LIBRERIA PIROLA MESSINA
Corso Cavour, 55
◇ **PALERMO**
LIBRERIA S.F. FLACCOVIO
Via Ruggero Settimo, 37
LIBRERIA FORENSE
Via Maqueda, 185
LIBRERIA S.F. FLACCOVIO
Piazza V. E. Orlando, 15-19
LIBRERIA MERCURIO LI.CA.M.
Piazza S. G. Bosco, 3
LIBRERIA DARIO FLACCOVIO
Viale Ausonia, 70
LIBRERIA CICALA INGUAGGIATO
Via Villaermosa, 28
LIBRERIA SCHOOL SERVICE
Via Galletti, 225
◇ **S. GIOVANNI LA PUNTA**
LIBRERIA DI LORENZO
Via Roma, 259
◇ **SIRACUSA**
LA LIBRERIA DI VALVO E SPADA
Piazza Euripide, 22
◇ **TRAPANI**
LIBRERIA LO BUE
Via Cascio Cortese, 8
LIBRERIA GIURIDICA DI SAFINA
Corso Italia, 81

TOSCANA

◇ **AREZZO**
LIBRERIA PELLEGRINI
Via Cavour, 42
◇ **FIRENZE**
LIBRERIA PIROLA «già Etruria»
Via Cavour, 46/R
LIBRERIA MARZOCCO
Via de' Martelli, 22/R
LIBRERIA ALFANI
Via Alfani, 84-86/R
◇ **GROSSETO**
NUOVA LIBRERIA
Via Mille, 6/A
◇ **LIVORNO**
LIBRERIA AMEDEO NUOVA
Corso Amedeo, 23-27
LIBRERIA IL PENTAFOGLIO
Via Fiorenza, 4/B
◇ **LUCCA**
LIBRERIA BARONI ADRI
Via S. Paolino, 45-47
LIBRERIA SESTANTE
Via Montanara, 37
◇ **MASSA**
LIBRERIA IL MAGGIOLINO
Via Europa, 19
◇ **PISA**
LIBRERIA VALLERINI
Via dei Mille, 13
◇ **PISTOIA**
LIBRERIA UNIVERSITARIA TURELLI
Via Macallè, 37
◇ **PRATO**
LIBRERIA GORI
Via Ricasoli, 25
◇ **SIENA**
LIBRERIA TICCI
Via delle Terme, 5-7
◇ **VIAREGGIO**
LIBRERIA IL MAGGIOLINO
Via Puccini, 38

TRENTINO-ALTO ADIGE

◇ **TRENTO**
LIBRERIA DISERTORI
Via Diaz, 11

UMBRIA

◇ **FOLIGNO**
LIBRERIA LUNA
Via Gramsci, 41
◇ **PERUGIA**
LIBRERIA SIMONELLI
Corso Vannucci, 82
LIBRERIA LA FONTANA
Via Sicilia, 53
◇ **TERNI**
LIBRERIA ALTEROCCA
Corso Tacito, 29

VENETO

◇ **BELLUNO**
LIBRERIA CAMPDEL
Piazza Martiri, 27/D
◇ **CONEGLIANO**
LIBRERIA CANOVA
Via Cavour, 6/B
◇ **PADOVA**
LIBRERIA DIEGO VALERI
Via Roma, 114
◇ **ROVIGO**
CARTOLIBRERIA PAVANELLO
Piazza V. Emanuele, 2
◇ **TREVISO**
CARTOLIBRERIA CANOVA
Via Calmaggiore, 31
◇ **VENEZIA**
CENTRO DIFFUSIONE PRODOTTI
EDITORIALI I.P.Z.S.
S. Marco 1893/B - Campo S. Fantin
◇ **VERONA**
LIBRERIA L.E.G.I.S.
Via Adigetto, 43
LIBRERIA GROSSO GHELFI BARBATO
Via G. Carducci, 44
LIBRERIA GIURIDICA EDITRICE
Via Costa, 5
◇ **VICENZA**
LIBRERIA GALLA 1880
Corso Palladio, 11

MODALITÀ PER LA VENDITA

La «Gazzetta Ufficiale» e tutte le altre pubblicazioni ufficiali sono in vendita al pubblico:

— presso l'Agenzia dell'Istituto Poligrafico e Zecca dello Stato in ROMA: piazza G. Verdi, 10;

— presso le Librerie concessionarie indicate nelle pagine precedenti.

Le richieste per corrispondenza devono essere inviate all'Istituto Poligrafico e Zecca dello Stato - Direzione Marketing e Commerciale - Piazza G. Verdi, 10 - 00100 Roma, versando l'importo, maggiorato delle spese di spedizione, a mezzo del c/c postale **n. 16716029.** Le inserzioni, come da norme riportate nella testata della parte seconda, si ricevono con pagamento anticipato, presso le agenzie in Roma e presso le librerie concessionarie.

PREZZI E CONDIZIONI DI ABBONAMENTO - 2000

Gli abbonamenti annuali hanno decorrenza dal 1° gennaio e termine al 31 dicembre 2000
i semestrali dal 1° gennaio al 30 giugno 2000 e dal 1° luglio al 31 dicembre 2000

PARTE PRIMA - SERIE GENERALE E SERIE SPECIALI
Ogni tipo di abbonamento comprende gli indici mensili

Tipo A - Abbonamento ai fascicoli della serie generale, inclusi tutti i supplementi ordinari:
- annuale .... **L. 508.000**
- semestrale .... **L. 289.000**

Tipo A1 - Abbonamento ai fascicoli della serie generale, inclusi i supplementi ordinari contenenti i provvedimenti legislativi:
- annuale .... **L. 416.000**
- semestrale .... **L. 231.000**

Tipo A2 - Abbonamento ai supplementi ordinari contenenti i provvedimenti non legislativi:
- annuale .... **L. 115.500**
- semestrale .... **L. 69.000**

Tipo B - Abbonamento ai fascicoli della serie speciale destinata agli atti dei giudizi davanti alla Corte costituzionale:
- annuale .... **L. 107.000**
- semestrale .... **L. 70.000**

Tipo C - Abbonamento ai fascicoli della serie speciale destinata agli atti delle Comunità europee:
- annuale .... **L. 273.000**
- semestrale .... **L. 150.000**

Tipo D - Abbonamento ai fascicoli della serie speciale destinata alle leggi ed ai regolamenti regionali:
- annuale .... **L. 106.000**
- semestrale .... **L. 68.000**

Tipo E - Abbonamento ai fascicoli della serie speciale destinata ai concorsi indetti dallo Stato e dalle altre pubbliche amministrazioni:
- annuale .... **L. 267.000**
- semestrale .... **L. 145.000**

Tipo F - *Completo.* Abbonamento ai fascicoli della serie generale, inclusi i supplementi ordinari contenenti i provvedimenti legislativi e non legislativi ed ai fascicoli delle quattro serie speciali (ex tipo F):
- annuale .... **L. 1.097.000**
- semestrale .... **L. 593.000**

Tipo F1 - Abbonamento ai fascicoli della serie generale inclusi i supplementi ordinari contenenti i provvedimenti legislativi ed ai fascicoli delle quattro serie speciali (escluso il tipo A2):
- annuale .... **L. 982.000**
- semestrale .... **L. 520.000**

Integrando con la somma di **L. 150.000** *il versamento relativo al tipo di abbonamento della* Gazzetta Ufficiale - *parte prima - prescelto, si riceverà anche l'Indice repertorio annuale cronologico per materie 2000.*

Prezzo di vendita di un fascicolo separato della *serie generale*	**L.**	**1.500**
Prezzo di vendita di un fascicolo separato delle *serie speciali I, II e III*, ogni 16 pagine o frazione	**L.**	**1.500**
Prezzo di vendita di un fascicolo della *IV serie speciale «Concorsi ed esami»*	**L.**	**2.800**
Prezzo di vendita di un fascicolo *indici mensili,* ogni 16 pagine o frazione	**L.**	**1.500**
Supplementi ordinari per la vendita a fascicoli separati, ogni 16 pagine o frazione	**L.**	**1.500**
Supplementi straordinari per la vendita a fascicoli, ogni 16 pagine o frazione	**L.**	**1.500**

Supplemento straordinario «Bollettino delle estrazioni»

Abbonamento annuale	**L.**	**162.000**
Prezzo di vendita di un fascicolo, ogni 16 pagine o frazione	**L.**	**1.500**

Supplemento straordinario «Conto riassuntivo del Tesoro»

Abbonamento annuale	**L.**	**105.000**
Prezzo di vendita di un fascicolo separato	**L.**	**8.000**

Gazzetta Ufficiale su MICROFICHES - 2000
(Serie generale - Supplementi ordinari - Serie speciali)

Abbonamento annuo (52 spedizioni raccomandate settimanali)	**L.**	**1.300.000**
Vendita singola: ogni microfiches contiene fino a 96 pagine di Gazzetta Ufficiale	**L.**	**1.500**
Contributo spese per imballaggio e spedizione raccomandata (da 1 a 10 microfiches)	**L.**	**4.000**

N.B. — Per l'estero i suddetti prezzi sono aumentati del 30%.

PARTE SECONDA - INSERZIONI

Abbonamento annuale	**L.**	**474.000**
Abbonamento semestrale	**L.**	**283.000**
Prezzo di vendita di un fascicolo, ogni 16 pagine o frazione	**L.**	**1.550**

I prezzi di vendita, in abbonamento ed a fascicoli separati, per l'estero*, nonché quelli di vendita dei fascicoli delle* annate arretrate*, compresi i fascicoli dei supplementi ordinari e straordinari, sono* raddoppiati.

L'importo degli abbonamenti deve essere versato sul c/c postale **n. 16716029** intestato all'Istituto Poligrafico e Zecca dello Stato. L'invio dei fascicoli disguidati, che devono essere richiesti entro 30 giorni dalla data di pubblicazione, è subordinato alla trasmissione dei dati riportati sulla relativa fascetta di abbonamento.

Per informazioni, prenotazioni o reclami attinenti agli abbonamenti oppure alla vendita della *Gazzetta Ufficiale* bisogna rivolgersi direttamente all'Amministrazione, presso l'Istituto Poligrafico e Zecca dello Stato - Piazza G. Verdi, 10 - 00100 ROMA

Ufficio abbonamenti	Vendita pubblicazioni	Ufficio inserzioni	Numero verde
☎ 06 85082149/85082221	☎ 06 85082150/85082276	☎ 06 85082146/85082189	☎ 800-864035